TOPOLOGICAL GROUPS

PRINCETON MATHEMATICAL SERIES

Editors: MARSTON MORSE, H. P. ROBERTSON, A. W. TUCKER

TOPOLOGICAL GROUPS

BY

L. PONTRJAGIN

PROFESSOR AT THE
STATE UNIVERSITY OF MOSCOW

TRANSLATED FROM THE RUSSIAN

BY

EMMA LEHMER

PRINCETON · 1946
PRINCETON UNIVERSITY PRESS
LONDON: HUMPHREY MILFORD
OXFORD UNIVERSITY PRESS

Printed in the United States of America

PREFACE

The concept of a continuous, or what is the same thing, topological group, arose in mathematics from the study of groups of continuous transformations. A group of continuous transformations, e.g. geometric transformations, constitutes in a natural way a topological manifold. It appeared later that for the treatment of the greater part of the problems arising in this connection it is not necessary to consider a group as a group of transformations, but merely to study the group intrinsically, remembering however that there is defined in it an operation of passage to a limit. Thus arose a new mathematical concept—topological group.

From a purely logical point of view the topological group is simply a combination of two fundamental mathematical concepts, group and topological space. Therefore the axiomatization of the concept of topological group is a natural procedure. In considering groups we study in purest form the algebraic operation of multiplication, while in considering topological spaces we investigate in just as pure a form the operation of passage to a limit. Since both these operations are among the fundamental operations of mathematics, they often occur together. The topological group is precisely that concept in which these two operations are united and interrelated. From the constructive point of view the axiomatization of topological groups is not interesting since in substance it is the same as for abstract groups. The first steps of the theory of topological groups are likewise devoid of specific interest. We devote the third chapter of this book to the exposition of this almost trivial part of the theory. In the first two chapters we have collected such information about groups and abstract spaces as will be needed throughout the book.

Once we possess the axiomatization and general theory of topological groups we come to a more interesting problem: to give a constructive development of this new abstract concept, i.e. to correlate it with older and more concrete concepts. In doing this new light is thrown from the new and more general point of view on the old concrete concepts, and at the same time the new abstract concept becomes more concrete. This is where the theory of representations, given in the fourth chapter of the book, plays a leading part. Indeed this theory enables us to study in detail the structure of compact topological groups and commutative ones. This is done in the seventh and fifth chapters.

One of the concrete concepts of the theory of topological groups is the concept of Lie group. In fact the theory of topological groups first arose in the theory of Lie groups. As is usual in relatively older theories, the theory of Lie groups left unsolved some of its fundamental problems. We devote the sixth chapter of this book to the solution of these problems. We also give there the required preliminary material for the seventh chapter since we investigate compact topological groups by means of their relation to Lie groups. The lat-

ter are investigated in greater detail in the ninth chapter where we give the foundation of the theory of Lie groups and formulate without proof certain results whose proofs are too complicated to be included. In the eighth chapter we define the concept of a universal covering group, which establishes a link between local properties of topological groups and their properties in the large.

Almost every section of this book ends in examples of various kinds—nearly trivial illustrations of the theoretical material on the one hand and on the other short proofs of theorems which are of interest in themselves.

The book need not be read in order. The interdependence of chapters is explained by the plan at the end of the table of contents.

The book is intended for the reader with rather modest mathematical preparation. On the whole we merely presuppose the knowledge of quite elementary mathematical material such as analytic geometry, theory of matrices, theory of ordinary differential equations, etc. Besides this elementary information, the book makes use of the following less elementary material:

1) The theory of integral equations, needed for Chapter IV. As a reference we may recommend W. V. Lovitt's *Linear Integral Equations*, New York, McGraw-Hill, 1924.

2) The theory of partial differential equations, in particular the conditions for solvability of equations in total differentials, this being needed for Chapter IX. As a reference we may recommend the chapter on this subject in de la Vallée-Poussin's *Cours d'Analyse infinitésimale*, vol. 2.

All necessary material along the lines just mentioned will be precisely formulated in the book in the form of theorems given without proof.

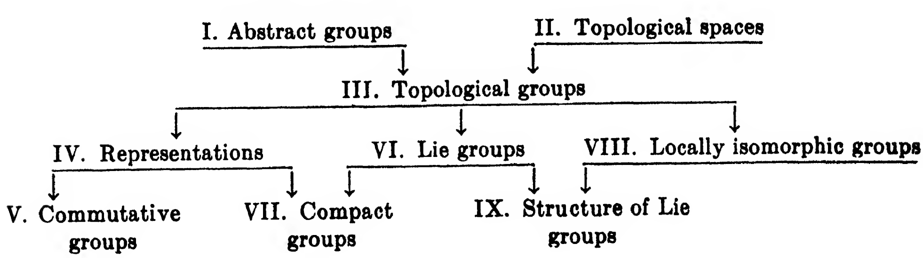
Numbers written in square brackets throughout the book refer to the bibliographical list at the end.

L. PONTRJAGIN

*The V. A. Stekloff Mathematical Institute
of the Academy of Sciences of the U.S.S.R.*

CONTENTS

INTERDEPENDENCE OF CHAPTERS



BASIC NOTATION

The notion of *set* or aggregate is fundamental in the exposition of this book, and it is assumed as known. We shall give here some definitions connected with the concept of set and with elementary operations on sets.

A) The notation $a \varepsilon M$ means that the element a belongs to the set M. If the set M is finite or countable, it will sometimes be given simply by enumerating its constituent elements. In symbols we would write $M = a_1, a_2, \cdots, a_n, \cdots$, which means that the set M is composed of the elements $a_1, a_2, \cdots, a_n, \cdots$.

B) The notation $M = N$ implies that M and N coincide.

C) The notation $M \subset N$ or $N \supset M$ means that every element of the set M is contained in the set N, i.e., that the set M is a subset of the set N. Here the possibility of the equality of M and N is not excluded.

D) $M \cap N$ denotes the *intersection* of the sets M and N, i.e. the set composed of all the elements which belong simultaneously to both M and N.

E) $M \cup N$ denotes the *sum* of the sets M and N, i.e. the set composed of all elements which belong to at least one of the sets M and N.

F) $M - N$ denotes the *difference* between the set M and the set N, i.e. the set composed of all the elements of M which are not contained in N. Defined in this way the operation of subtraction is always possible, whether the set N is a subset of the set M or not. If $M \subset N$ the result of subtraction is the null set, i.e. the set which contains no elements.

G) Let M and N be two sets. Suppose that to each element x of the set M there corresponds a definite element $y = f(x)$ of the set N. We shall then say that there exists a *mapping* f of the set M *in* the set N. The element y is called the *image* of the element x under the mapping f, while the element x is the inverse image or one of the inverse images of the element y.

We say that f is a mapping of the set M *on* the set N if each element y of the set N has at least one inverse image x under the mapping f, i.e. for each y there is at least one x such that $y = f(x)$.

If A is a subset of the set M, i.e. $A \subset M$, then by $f(A)$ we shall designate the set of all those elements of N which are images of the elements of A, and we shall call $F(A)$ the *image* of the set A. If $B \subset N$, we shall designate by $f^{-1}(B)$ the set of all those elements of M which go over into the set B under the mapping f. We shall call the set $f^{-1}(B)$ the *complete inverse image* of the set B under the mapping f.

The mapping f of the set M on the set N is called *one-to-one* if every element of the set N has a unique inverse image under the mapping f. If f is one-to-one the equation $y = f(x)$ can be solved for x, i.e. given y we can determine x uniquely; we express the solution as $x = f^{-1}(y)$. The mapping f^{-1} is called the *inverse* of f.

CHAPTER I

ABSTRACT GROUPS

The theory of abstract groups investigates an algebraic operation in its purest form. The elements which compose the group are considered only from the point of view of the group operation; all other aspects of these elements are laid aside.

The present chapter is dedicated to the exposition of the fundamental concepts of the theory of abstract groups.

1. The Concept of a Group

DEFINITION 1. A set G of elements is called a *group* if the following conditions, known as *group axioms*, are satisfied:

1) There exists an operation in G which associates with each pair of elements a, b of G a third element c of G. This operation is usually called *multiplication* and the element c is called the *product* of a and b, written $c = ab$. (The product ab may depend on the order of the factors a and b; ab, in general is not equal to ba.)

2) The multiplication is *associative*, i.e., if a, b, and c are any three elements of G, then $(ab)c = a(bc)$.

3) The group G contains a *right identity*, which is the same for all elements of the group, i.e., an element e such that $ae = a$ for every element a of G.

4) For each element a of G there exists a *right inverse* element, i.e., an element a^{-1} such that $aa^{-1} = e$.

The set of elements of the group G can be either finite or infinite. If the set G is finite, then the group itself is also called *finite*, and the number of elements of the group G is called the *order* of the group G. Otherwise the group G is called *infinite*.

If besides the four axioms given above the group also satisfies the commutative law, i.e., if for any two elements a and b of G it is true that

$$ab = ba, \tag{1}$$

then the group is called *commutative* or *abelian*.

In abelian groups the multiplicative notation is often replaced by additive notation, i.e., instead of the product ab we write the *sum* $a + b$, in which case the group operation is called *addition* instead of multiplication. The identity e is then called *zero* and denoted by 0, and the element a^{-1}, the inverse of a, is called the *negative* of a and denoted by $-a$.

A) Since by axiom 2) $(ab)c = a(bc)$ we designate this element simply by abc. In exactly the same way a product of four elements, say $((ab)c)d$, can be written simply as $abcd$, for, as can be seen easily, this product does not depend on the

distribution of parentheses. The same rule holds for the product of any number of factors.

B) A right identity e of a group is likewise a *left identity*, i.e., $ea = a$ for every element a. A right inverse element a^{-1} of the element a is also a left inverse element, i.e., $a^{-1}a = e$. An element inverse to the element a^{-1} coincides with the element a, i.e., $(a^{-1})^{-1} = a$.

We shall now prove B). It follows from axioms 3) and 4) that $a^{-1}aa^{-1} = a^{-1}$. Multiplying this equation on the right by the right inverse of the element a^{-1}, we get $a^{-1}a = e$, i.e., the right inverse is a left inverse. This also shows that the element inverse to a^{-1} is a. Moreover we see that $ea = aa^{-1}a = ae = a$, i.e., a right identity is also a left identity.

C) In the group G each of the equations

$$ax = b \tag{2}$$

and

$$ya = b \tag{3}$$

has a unique solution with respect to the unknowns x and y. From this follows, in particular, the uniqueness of the identity and of the inverse element, since e is the solution of the equation $ax = a$, and the element a^{-1} is the solution of $ax = e$.

To establish the solvability of (2) and (3) it is sufficient to point out that the element $a^{-1}b$ is a solution of (2), while the element ba^{-1} satisfies (3). It is obvious that the above solutions are unique, for multiplying (2) on the left by a^{-1} we get $x = a^{-1}b$, while multiplying (3) on the right by a^{-1} we obtain $y = ba^{-1}$.

D) After we have proved the uniqueness of the identity and of the inverse element (see C)), it is natural to introduce the notations of elementary algebra. If m is a natural number, then a^{m+1} is determined by induction from the equation $a^{m+1} = a^m a$, with $a^1 = a$. We determine negative powers of a by defining $a^{-m} = (a^{-1})^m$, while $a^0 = e$. If p and q are two integers, it is easy to show that the ordinary rules of algebra hold, namely: $a^p a^q = a^{p+q}$, $(a^p)^q = a^{pq}$. In the additive notation we write na for a^n.

E) We shall say that an element a of a group is of *finite order* if there exists a natural number m such that $a^m = e$. Otherwise we ascribe to the element a an infinite or zero order, or we say that the element a is *free*.

If the element a is of finite order, then we take for the numerical value of this order the least natural number r for which $a^r = e$. It turns out that if $a^n = e$ for an integer n, then n is divisible by r. To prove this assertion let us divide n by r, i.e., write n in the form $n = pr + q$, where q is the remainder on division, and

$$0 \leqq q < r. \tag{4}$$

Then we have $e = a^n = a^{pr+q} = (a^r)^p a^q = a^q$. Hence $a^q = e$ and, therefore, from the inequality (4), $q = 0$, i.e., n is divisible by r.

EXAMPLE 1. Let M be a set. We shall call any one-to-one mapping of the set M onto itself a *transformation* of the set M. If s is a transformation of M, then every element a of M is associated with some definite element $s(a)$ of M. The result of the transformation s as applied to a is also written sa, $s(a) = sa$.

The aggregate G of all the transformations of the set M forms a group. Let s and t be two transformations of M. We shall define their product $r = st$ by means of the condition $r(a) = s(t(a))$ for every element a of M. It is easy to see that we have so determined r that it is a one-to-one mapping of M onto itself.

The law of multiplication of transformations given above is associative since $(rs)t = r(st)$. To prove this we operate with both sides of this equation on an arbitrary element a of M:

$$(rs)t(a) = (rs)(t(a)) = r(s(t(a))),$$

$$r(st)(a) = r(st(a)) = r(s(t(a))),$$

i.e., in both cases we get the same result.

The identity of the group G of transformations of the set M is the identity transformation, i.e., a transformation e under which every element a of M is transformed into itself, $e(a) = a$. The inverse of the transformation s is the transformation s^{-1} which transforms every element $s(a)$ of the set M into a. Since the transformation s is a one-to-one mapping, it follows that every element of M can be written in the form $s(a)$ and therefore the transformation s^{-1} is determined for all the elements of the set M.

Hence all the axioms of a group are satisfied by the set G of transformations.

Let H be an aggregate of transformations of the set M which need not contain all the transformations of M. H forms a group by virtue of the same law of multiplication which operates in G if H contains the product of any two transformations of H and also contains the inverse of every transformation of H.

EXAMPLE 2. Let G be the totality of all n-rowed square matrices $\|s_j^i\|$ whose elements are real numbers and whose determinant is different from zero. We define as the product of two matrices $\|s_j^i\|$ and $\|t_j^i\|$ the matrix $\|r_j^i\|$, where

$$r_j^i = \sum_{k=1}^{n} s_k^i t_j^k.$$

The group G defined in this way can be regarded as the group of all linear transformations of the n-dimensional Euclidean space R^n which leave fixed a certain point 0. Let the point 0 be the origin of our coordinate system, and let a be any point of R^n with coordinates a^i, $i = 1, 2, \cdots, n$. Denote by $s(a)$ the point whose coordinates are $b^i = \sum_{k=1}^{n} s_k^i a^k$, $i=1, 2, \cdots, n$. We thus obtain a one-to-one mapping s of the space R^n into itself. In fact if we regard the last set of equalities as a system of linear equations with respect to a^k, then this system has a unique solution since the determinant $|s_k^i| \neq 0$.

It is easily seen that if s and t are two transformations of the space R^n determined by the matrices $\|s_j^i\|$ and $\|t_j^i\|$, then the product $st = r$ is determined by the matrix $\|r_j^i\|$ which is the product of the matrices $\|s_j^i\|$ and $\|t_j^i\|$. We have proved in example 1 that the totality of transformations obeys the associative law. Hence, the associative law holds in the totality of matrices discussed above.

The identity of the group of matrices is the unit matrix $\|\delta_j^i\|$, $\delta_i^i = 1$, $\delta_j^i = 0$, for $i \neq j$. In order to find the matrix $\|t_j^i\|$ inverse to the matrix $\|s_j^i\|$, it is sufficient to solve the system of equations $\sum_{k=1}^n s_k^i t_j^k = \delta_j^i$. Since the determinant $|s_k^i| \neq 0$, this system of equations has a solution.

2. Subgroup. Normal Subgroup. Factor Group

In what follows we shall frequently have to consider different subsets of a group, and several operations on these subsets. We give here a notation for these operations.

A) If A and B are two subsets of a group G, we denote by AB the subset composed of all the elements of the form xy, where $x \varepsilon A$, $y \varepsilon B$. We denote by A^{-1} the subset composed of all the elements of the form x^{-1}, where $x \varepsilon A$. For a natural number m we determine the subset A^{m+1} by induction from $A^{m+1} = A^m A$ with $A^1 = A$. The subset A^{-m} is determined by letting $A^{-m} = (A^{-1})^m$, while the subset $A^0 = \{e\}$. The notation above enables us to form the product of any number of subsets raised to arbitrary integral powers. In what follows we shall sometimes fail to distinguish between a set containing a single element, and that element itself. It therefore makes sense to write Ab, where $A \subset G$, $b \varepsilon G$. We note that if A is not the null set, then

$$AG = GA = G \tag{1}$$

$$G^{-1} = G \tag{2}$$

$$Ae = eA = A. \tag{3}$$

Using the additive notation we would write $A + B$ for AB and nA for A^n.

Given a group G we can construct from it other groups. The easiest construction is the following:

Definition 2. A set H of elements of a group G is called a *subgroup* of G if H forms a group under the same law of multiplication which operates in G.

B) In order that the subset H of the group G be a subgroup it is necessary and sufficient that one of the two following conditions be fulfilled:

a) If H contains any two elements a and b, it must contain the element ab^{-1}. Making use of the notation in A) this condition can be written in the form

$$HH^{-1} \subset H. \tag{4}$$

b) If H contains any two elements a and b, it must contain the element ab and the element a^{-1}. In symbols this condition can be written

$$H^2 \subset H \tag{5}$$

and

(6) $$H^{-1} \subset H.$$

The necessity of the above conditions is obvious. We shall now prove their sufficiency. If $a \varepsilon H$, then by a) we have $aa^{-1} = e \varepsilon H$. Further since $e \varepsilon H$ and $a \varepsilon H$ it follows from condition a) that $ea^{-1} = a^{-1} \varepsilon H$. If a and b are two elements of H, then $b^{-1} \varepsilon H$, and therefore from a) we have $ab = a(b^{-1})^{-1} \varepsilon H$. Therefore, if the condition a) is satisfied, H is a subgroup. The proof of the sufficiency of b) is quite analogous.

Every group contains as one of its subgroups the set consisting of all integral powers of a given element. A group which consists exclusively of integral powers of one of its elements is called *cyclic*. Infinite cyclic groups are called *free* groups; all their elements (with the exception of the identity) are free (see §1, E)).

In constructing new concepts modern mathematics often makes use of a relation of equivalence, which can be formulated as follows:

C) We say that a *relation of equivalence* has been established in a set M if it is possible to assert whether any two elements a, b of M are equivalent or not, in symbols $a \sim b$ or a not $\sim b$, where the relation of equivalence is

a) reflexive: $a \sim a$;

b) symmetric: If $a \sim b$, then $b \sim a$,

c) transitive: If $a \sim b$ and $b \sim c$, then $a \sim c$.

If the above conditions hold, then the relation of equivalence established in M automatically divides M into disjoint classes of equivalent elements.

Let us now apply this general concept of equivalence to groups.

D) Let G be a group and H a subgroup. If a and b are two elements of G, then we shall say that $a \sim b$ if and only if $ab^{-1} \varepsilon H$. It turns out that this relation of equivalence established in G satisfies the conditions of Definition C), and therefore G is divided into classes of equivalent elements. Each of the classes thus obtained is called a *right coset* of the subgroup H relative to the group G. It turns out that if A is a right coset of the subgroup H and if $a \varepsilon A$, then $A = Ha$ (see §2, A)); moreover, every subset of the form Hb is a right coset. Since $H = He$, the subgroup H itself is one of the cosets.

We shall show first of all that the relation of equivalence given in D) satisfies the conditions of definition C).

First $a \sim a$, since $aa^{-1} = e \varepsilon H$. If $a \sim b$, then $ab^{-1} \varepsilon H$; hence $(ab^{-1})^{-1} = ba^{-1} \varepsilon H$, so that $b \sim a$. If $a \sim b$ and $b \sim c$, then $ab^{-1} \varepsilon H$ and $bc^{-1} \varepsilon H$; hence $ac^{-1} = ab^{-1}bc^{-1} \varepsilon H$, that is $a \sim c$. Thus all three conditions are satisfied.

We show further that if A is any right coset of the subgroup H and if $a \varepsilon A$, then $A = Ha$. In fact, let $x \varepsilon A$; then $xa^{-1} \varepsilon H$, and hence $x \varepsilon Ha$. If $y \varepsilon Ha$, then $ya^{-1} \varepsilon H$, and hence $y \varepsilon A$.

Finally we prove that every set Hb is a coset. In fact, the element b belongs to one of the cosets, say B, and, therefore, from what we have just proved, $B = Hb$.

Hence D) is established.

E) Besides the definition of equivalence given in D), we can give another entirely analogous definition by saying that $a \sim b$ if and only if $a^{-1}b \varepsilon H$. The classes obtained in this way are called *left cosets* of the subgroup H. Just as in D), it can be proved that every left coset can be written in the form aH, and conversely every subset of the form bH is a left coset.

We shall now ask under what conditions the right and left cosets of the subgroup H coincide. If A is both a right and a left coset of H, then $A = Ha = aH$, where $a \varepsilon A$. If every right coset is also a left coset, then $Ha = aH$ for every $a \varepsilon G$. Multiplying the last relation on the left by a^{-1} we get $a^{-1}Ha = H$. Subgroups which possess this property are characterized by the following property.

DEFINITION 3. A subgroup N of a group G is called an *invariant* or *normal subgroup* of G if for every $n \varepsilon N$ and every $a \varepsilon G$ we have $a^{-1}na \varepsilon N$, or what is the same, $a^{-1}Na \subset N$ for every $a \varepsilon G$.

If N is a normal subgroup, i.e., $a^{-1}Na \subset N$ for every $a \varepsilon G$, then $a^{-1}Na = N$ for every $a \varepsilon G$. In fact, let $a = b^{-1}$; we then have $bNb^{-1} \subset N$. Multiplying this relation on the left by b^{-1} and on the right by b we get $N \subset b^{-1}Nb$. But since a was arbitrary, b is an arbitrary element of G, and therefore $b^{-1}Nb = N$ for an arbitrary $b \varepsilon G$. The last relation can be written

$$Nb = bN. \tag{7}$$

F) In order that the right and left cosets of the subgroup N coincide it is necessary and sufficient that N be a normal subgroup.

The necessity of this condition was shown above. We shall now prove the sufficiency. If A is a right coset of N, then $A = Na$, but $Na = aN$ (see (7)), and therefore A is a left coset.

The following definition gives a second method for the construction of groups from a given group G.

DEFINITION 4. Let N be a normal subgroup of the group G, and let A and B be two cosets of N, $A = Na$, $B = Nb$. We form the product AB (see A)), and obtain $AB = NaNb = NNab = Nab$, that is, the product AB is also a coset of N. Thus we have established a law of multiplication in the totality of cosets, and, as we shall show presently, this multiplication satisfies the group axioms. The set of all cosets thus obtained is called the *factor group* of G by the normal subgroup N and is denoted by G/N.

We shall show that the axioms 2), 3), and 4) of Definition 1 are satisfied in G/N.

Associativity is obvious, as it holds in G. The identity of the group G/N is N. For if aN is a coset, then $(aN)N = aN$. The inverse of Na is $a^{-1}N$, for $(Na)(a^{-1}N) = N$.

G) Every group G has at least two normal subgroups, namely the subgroup consisting only of the identity, and the subgroup which coincides with the

group G. If G has no normal subgroups other than these two trivial ones, G is called a *simple* group.

EXAMPLE 3. Let G be the group of all transformations of the set M (see Example 1), and let a be an element of M. Let us denote by H the totality of all transformations which leave a fixed. It is easy to see that H is a subgroup of G.

If M contains more than two elements, then H is not a normal subgroup of G. In the first place $H \neq G$. In fact, let $b \in M$, where $b \neq a$. We shall now determine the transformation t by means of the conditions $t(a) = b$ and $t(b) = a$, while $t(x) = x$ if $x \neq a$ and $x \neq b$. Further let b' be an element of M different from a and b. Such an element exists since M is supposed to contain more than two elements. We now determine a transformation s by prescribing $s(b) = b'$, $s(b') = b$; for all other elements, s is the identity. Then $s(a) = a$, that is $s \in H$. Consider now $t^{-1}st(a)$: we have $t^{-1}st(a) = t^{-1}s(b) = t^{-1}(b') = b'$, and therefore $t^{-1}st$ is not an element of H.

EXAMPLE 4. Let G be the group of matrices of example 2. The set H of all orthogonal matrices (see below) forms a subgroup of the group G. Let us consider the matrix $s = \|s_j^i\|$. The matrix $t = \|t_j^i\|$ determined by $t_i^j = s_j^i$ is called the *transpose* of s and is denoted by s^*, $t = s^*$. The matrix s is called *orthogonal* if $ss^* = \|\delta_j^i\| = e$.

It is obvious that the unit matrix $\|\delta_j^i\| = e$ is orthogonal, and $e \in H$. If s is an orthogonal matrix, then $s^{-1} = s^*$, since $ss^* = e$. We shall show that s^* is also orthogonal. The tranpose of s^* is s, i.e., $s^{**} = s$. Hence $s^*s^{**} = s^*s$. But since $s^* = s^{-1}$, it follows that $s^*s^{**} = e$, i.e., $s^{-1} = s^*$ is an orthogonal matrix. Hence if s is in H, so is s^{-1}. Now let s and t be two matrices. It is easy to see that $(st)^* = t^*s^*$. If s and t are orthogonal, we have $(st)(st)^* = stt^*s^* = e$, i.e., the matrix st is also orthogonal. Therefore if s and t are matrices in H, so is their product st. Hence H is a subgroup of G. It is easy to show that H is not an invariant subgroup of the group G.

EXAMPLE 5. Let G be the group of matrices given in example 2. Denote by H the aggregate of all those matrices in G whose determinant is unity. Since in multiplying matrices the associated determinants are also multiplied, it is not hard to see that H is a normal subgroup of the group G.

3. Isomorphism. Automorphism. Homomorphism

We pointed out at the beginning of this chapter that the abstract theory of groups considers a group only from the point of view of the group operation. This situation is clearly expressed in the following definition.

DEFINITION 5. A mapping f of a group G on a group G' is called *isomorphic* or an *isomorphism*, if it is

1) one-to-one, and

2) such that the operation of multiplication is preserved, i.e., $f(xy) = f(x)f(y)$ for any two elements x, y, of G.

It is easy to see that if the mapping f is isomorphic then its inverse mapping f^{-1} is also isomorphic.

Two groups G and G' are called *isomorphic* if there exists an isomorphic mapping of one group upon the other.

If two groups G and G' are isomorphic, then they are identical from the point of view of abstract group theory. In other words, the theory of abstract groups studies only those properties and concepts which remain unchanged under isomorphic transformations.

A) Consider the isomorphic mappings of a group G onto itself. Such isomorphic mappings are called *automorphisms* of G. Since every automorphism of G is one-to-one, it follows that an automorphism of G is a transformation of G (see example 1). Hence two automorphisms can be multiplied, and the resulting product gives a transformation of the group G which is also an automorphism of G. It is clear, moreover, that the identity transformation is an automorphism, and that a transformation inverse to an automorphism is also an automorphism. Therefore the aggregate of all automorphisms of a group G forms a group.

B) Let a be a fixed element of the group G. We determine from it an automorphism f_a of the group G by letting

$$(1) \qquad f_a(x) = axa^{-1}$$

for every $x \varepsilon G$. The automorphism thus obtained is called an *inner* automorphism. The aggregate of all inner automorphisms of the group G forms a subgroup of the group of all automorphisms. Moreover

$$(2) \qquad f_af_b = f_{ab}.$$

Let us show that the relation (1) really gives an automorphism. First of all the mapping f_a has an inverse f_a^{-1} defined by

$$(3) \qquad f_a^{-1} = f_{a^{-1}}.$$

In fact $f_a\,(f_{a^{-1}}(x)) = a(a^{-1}xa)a^{-1} = x$, and therefore, f_a is one-to-one. Further

$$f_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = f_a(x)f_a(y).$$

To prove that the totality of all inner automorphisms forms a group one has only to prove (2), (see §2, B)). We have

$$f_a(f_b(x)) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = f_{ab}(x).$$

A relation between two groups which is weaker than the isomorphic mapping is established by the so-called homomorphic mapping.

Definition 6. A mapping g of a group G into a group G^* is called *homomorphic* or a *homomorphism* if it preserves the operation of multiplication, i.e., if

$$(4) \qquad g(xy) = g(x)g(y)$$

for any two elements x, y of G. The set of all the elements of the group G

which go into the identity of the group G^* under the homomorphism g is called the *kernel* of this homomorphism.

If g is a homomorphism of the group G into the group G^* then

$$g(e) = e^*, \tag{5}$$

i.e., the identity e of the group G goes into the identity e^* of the group G^*. Moreover

$$g(x^{-1}) = (g(x))^{-1} \tag{6}$$

for any $x \varepsilon G$. In fact $g(x)g(e) = g(xe) = g(x)$, so that $g(e) = e^*$. Further $g(x)g(x^{-1}) = g(xx^{-1}) = g(e) = e^*$, which means that $g(x^{-1}) = (g(x))^{-1}$.

The following theorem establishes the connection between homomorphic and isomorphic mappings.

THEOREM 1. *Let the group G be homomorphically mapped on the group G^* by a homomorphism g, and let N be the kernel of the homomorphism g. Then N is a normal subgroup of the group G and G^* is isomorphic with the group G/N* (see Definition 4).

This can be stated more explicitly as follows: *If x^* is an element of the group G^*, and X is the set of all elements of the group G which go into x^* under the homomorphism g, then X is a coset of the subgroup N, i.e., $X \varepsilon G/N$. The one-to-one relation thus obtained between the elements of the groups G/N and G^* is an isomorphism.*

We shall call this the *natural isomorphism* to distinguish it from other possible isomorphisms between the two groups.

PROOF. We shall show that N forms a group. If $x \varepsilon N$ and $y \varepsilon N$, it follows that $g(x) = e^*$, $g(y) = e^*$. Then $g(xy) = g(x)g(y) = e^*e^* = e^*$, i.e., $xy \varepsilon N$. Furthermore, if $x \varepsilon N$, then $g(x) = e^*$, but then (see (6)) $g(x^{-1}) = (g(x))^{-1} = e^{*-1} = e^*$, i.e., $x^{-1} \varepsilon N$. Therefore, (see §2, B)) N is a subgroup of the group G.

We show next that N is an invariant subgroup of the group G. Let $x \varepsilon N$ and $a \varepsilon G$, then $g(a^{-1}xa) = g(a^{-1})g(x)g(a) = (g(a))^{-1}e^*g(a) = e^*$, i.e., $a^{-1}xa \varepsilon N$.

Let a^* be an element of G^*, and A the totality of all the elements of G which map into a^* under the homomorphism g. If a and a' are two elements of A, then

$$g(a'a^{-1}) = g(a')g(a^{-1}) = g(a')(g(a))^{-1} = a^*a^{*-1} = e^*.$$

Hence $a'a^{-1} \varepsilon N$, i.e., a and a' belong to the same coset of N. Conversely, if x belongs to the same coset as a, that is, if $xa^{-1} \varepsilon N$, then $g(x)a^{*-1} = g(x)g(a^{-1}) = g(xa^{-1}) = e^*$, i.e., $g(x) = a^*$. Hence A forms a complete coset of N, and we have a one-to-one correspondence between cosets of N on the one hand and elements of G^* on the other. In fact, to every element a^* of G^* there corresponds a coset formed from all the elements which map into a^* under the homomorphism g. But every coset is an element of the group G/N (see Defini-

tion 4) and, therefore, to every element $A \varepsilon G/N$ there corresponds an element $f(A) = a^* \varepsilon G^*$, where f is a one-to-one mapping. We shall show that f is an isomorphic mapping. Let A and B be two elements of G/N, and $a \varepsilon A$, $b \varepsilon B$. Suppose that $g(a) = a^*$, $g(b) = b^*$; then $f(A) = a^*$, $f(B) = b^*$. Furthermore, $ab \varepsilon AB$; therefore

$$f(AB) = g(ab) = a^*b^* = f(A)f(B),$$

and the conditions for isomorphism are satisfied. Hence G^* and G/N are isomorphic.

The next proposition is closely connected with theorem 1.

C) Let G be a group, and N a normal subgroup of G. Construct the mapping g of the group G on the group G/N by associating with every element $x \varepsilon G$ that element $g(x) = X \varepsilon G/N$ which contains x, $x \varepsilon X$. The mapping of the group G on the group G/N which we thus obtain is homomorphic. We shall call this mapping the *natural homomorphism of a group on its factor group* to distinguish it from other possible homomorphisms.

Let a and b be two elements of G. Suppose that $a \varepsilon A \varepsilon G/N$, $b \varepsilon B \varepsilon G/N$. Then by definition

$$g(a) = A, \tag{7}$$

$$g(b) = B. \tag{8}$$

On the other hand $ab \varepsilon AB$, and therefore

$$g(ab) = AB. \tag{9}$$

Combining (7), (8), and (9) we get $g(ab) = g(a)g(b)$, which means that g is a homomorphism.

D) We note that if the homomorphism g has the identity for its kernel, i.e., $N = \{e\}$, then g is an isomorphism. In fact in this case there is mapped upon every element of G^* only one element of G, since every coset contains just one element.

E) If the homomorphism g maps the group G *in* (part of) the group G^* instead of *on* (all of) the group G^*, then the set of all the elements of G^* which are images of the elements of G forms a subgroup of the group G.*

Let us denote the above set by H^*. If x^* and y^* are two elements of H^*, then $x^* = g(x)$ and $y^* = g(y)$, and $x^*y^{*-1} = g(xy^{-1})$, i.e., $x^*y^{*-1} \varepsilon H^*$. Therefore, (see §2, B)) H^* is a subgroup of the group G^*.

F) Let g be a homomorphism of the group G on the group G^*. If H is a subgroup of G, then $g(H)$ is a subgroup of G^*. If H is a normal subgroup of the group G, then $g(H)$ is a normal subgroup of the group G^*.

The fact that $g(H)$ is a subgroup follows from proposition E), since g is a homomorphism of the group H in the group G^*. Let us consider the case where H is a normal subgroup. Let $x^* \varepsilon G^*$; then there exists an $x \varepsilon G$ such that $g(x) = x^*$. We have $x^{-1}Hx \subset H$, from which it follows that $x^{*-1}g(H)x^* = g(x^{-1}Hx) \subset g(H)$. Therefore $g(H)$ is a normal subgroup of the group G^*.

G) Let g be a homomorphism of the group G in the group G^*. Denote by $g^{-1}(H^*)$ the set of all those elements of G which go into $H^* \subset G^*$ under the homomorphism g. If H^* is a subgroup of the group G^*, then $g^{-1}(H^*)$ is a subgroup of the group G. If H^* is a normal subgroup of the group G^*, then $g^{-1}(H^*)$ is a normal subgroup of the group G.

Let H^* be a subgroup and let $a \varepsilon g^{-1}(H^*)$, $b \varepsilon g^{-1}(H^*)$. Then $g(ab^{-1}) = g(a)(g(b))^{-1} \varepsilon H^*$, i.e., $ab^{-1} \varepsilon g^{-1}(H^*)$. Hence (see §2, B)) $g^{-1}(H^*)$ is a subgroup. Let H^* be a normal subgroup, and $a \varepsilon g^{-1}(H^*)$, $x \varepsilon G$. Then $g(x^{-1}ax) = (g(x))^{-1}g(a)g(x) \varepsilon H^*$, i.e., $x^{-1}ax \varepsilon g^{-1}(H^*)$. Hence $g^{-1}(H^*)$ is a normal subgroup of the group G.

H) It is not hard to see that if g is a homomorphism of the group G on the group G^*, and g^* is a homomorphism of the group G^* on the group G^{**}, then the mapping $h(x) = g^*(g(x))$ is a homomorphism of the group G on the group G^{**}.

Example 6. Let G be the additive group of all real numbers, and G' the multiplicative group of all positive real numbers. The groups G and G' are isomorphic. Let us construct the isomorphic mapping $f(x) = e^x$ which assigns to every element $x \varepsilon G$ a corresponding element $f(x) \varepsilon G'$. Clearly the mapping $f(x)$ is one-to-one and is isomorphic, since $f(x + y) = f(x)f(y)$.

Example 7. Let G be the group of matrices given in example 2, and let G^* be the multiplicative group of all real numbers different from zero. We shall give a homomorphic mapping of the group G on G^*. If s is a matrix of G, we will suppose that $g(s) = |s|$, where $|s|$ is the determinant of the matrix s. Then we have $g(st) = |st| = |s||t|$. Moreover, G contains matrices with arbitrary determinants different from zero. Hence g is a homomorphic mapping of the group G *on* G^*. Since the identity of the group G^* is the number 1, the kernel of the homomorphism g is the totality of all matrices whose determinant is equal to unity.

4. Center. Commutator Subgroup

In this section we investigate the question of the dependence of the product on the order of its factors.

A) Two elements a and b of the group G are said to *commute* if their product does not depend on the order of the factors, $ab = ba$.

Definition 7. An element z of the group G is called *central* if it commutes with each element of the group G, i.e., $zx = xz$ for every $x \varepsilon G$, or equivalently, $x^{-1}zx = z$. The set Z of all central elements of the group G is called the *center* of the group G.

We shall now show that the center Z is a subgroup of the group G. In fact, if z and z' are two elements of Z, then for every $x \varepsilon G$, $xzz' = zxz' = zz'x$, that is $zz' \varepsilon Z$. We next raise both sides of the relation $xz = zx$ to the power -1, and obtain $z^{-1}x^{-1} = x^{-1}z^{-1}$, and on replacing x^{-1} by y we obtain $z^{-1}y = yz^{-1}$; but since x is an arbitrary element, y is also an arbitrary element, i.e., $z^{-1} \varepsilon Z$. Hence Z is a subgroup of the group G.

B) Every subgroup H of the group Z is a normal subgroup of the group G. In fact if $h \varepsilon H$, then $h \varepsilon Z$, and hence $x^{-1}hx = h \varepsilon H$ for every $x \varepsilon G$. In particular the center itself is a normal subgroup. The subgroups of the group Z are called *central normal subgroups*.

C) In order to settle the question whether the elements a and b commute or not, it is sufficient to form the product $ab(ba)^{-1} = aba^{-1}b^{-1}$; if this product is equal to unity, then a and b commute, if not, they do not commute. The product $aba^{-1}b^{-1}$ is called the *commutator* of a and b.

DEFINITION 8. Let us form the set Q of all the elements of the group G which can be written in the form $q_1q_2 \cdots q_m$, where each q_i is the commutator of some pair of elements of G. The set Q is called the *commutator subgroup* of the group G.

We shall show that the commutator subgroup Q of the group G is a normal subgroup of the group G.

Let x and y be two elements of Q, $x = q_1 \cdots q_m$, $y = q_1' \cdots q_n'$, where the factors on the right are commutators. Then $xy = q_1 \cdots q_mq_1' \cdots q_n'$, and therefore $xy \varepsilon Q$. If q is a commutator, then $q = aba^{-1}b^{-1}$, and $q^{-1} = bab^{-1}a^{-1}$, i.e., q^{-1} is also a commutator. Hence $x^{-1} = q_m^{-1} \cdots q_1^{-1}$ belongs to Q, and therefore Q is a subgroup of the group G. If $q = aba^{-1}b^{-1}$, then $c^{-1}qc = (c^{-1}ac)(c^{-1}bc)(c^{-1}ac)^{-1}(c^{-1}bc)^{-1}$. Hence $c^{-1}qc$ is also a commutator. If $x = q_1 \cdots q_m$, then $c^{-1}xc = (c^{-1}q_1c) \cdots (c^{-1}q_mc)$, and therefore $c^{-1}xc \varepsilon Q$ for every $c \varepsilon G$, and every $x \varepsilon Q$, and the proposition follows.

D) The factor group G/Q of the group G by its commutator subgroup Q is commutative; moreover, Q is the least normal subgroup of the group G which has this property, i.e., if G/N is commutative, then $Q \subset N$.

Let A and B be two cosets of Q. We form the product $AB\,A^{-1}B^{-1}$. This product contains a commutator, namely $aba^{-1}b^{-1}$, where $a \varepsilon A$, $b \varepsilon B$. Then, since $ABA^{-1}B^{-1}$ is a coset, we have $ABA^{-1}B^{-1} = Q$ (see Definition 4). Hence if we consider A and B as elements of the group G/Q, then $ABA^{-1}B^{-1}$ is the identity of this group, i.e., A and B commute in G/Q, and G/Q is a commutative group.

Let N be a normal subgroup of G such that $N \not\supset Q$. Then N cannot contain all the commutators of the group G; otherwise N would contain all the products of all the commutators, and so would contain Q. Let a and b be two elements of G such that $aba^{-1}b^{-1}$ is not an element of N. Denote by A and B the cosets of the subgroup N which contain a and b respectively. Then $aba^{-1}b^{-1}$ does not belong to N and therefore $ABA^{-1}B^{-1}$ is not the identity of the group G/N, i.e., A and B do not commute in G/N. Hence the group G/N is not commutative.

E) Let N be a normal subgroup of the group G and Q the commutator subgroup of N. Then Q is a normal subgroup of the group G.

It is obvious that Q is a subgroup of the group G Let q be a commutator of two elements of N, $q = aba^{-1}b^{-1}$, where $a \varepsilon N$, $b \varepsilon N$. Then we have for every $c \varepsilon G$, $c^{-1}qc = (c^{-1}ac)(c^{-1}bc)(c^{-1}ac)^{-1}(c^{-1}bc)^{-1}$, but since N is a normal

subgroup of G, $c^{-1}ac \in N$, $c^{-1}bc \in N$, i.e., $c^{-1}qc$ is a commutator of elements of N. Hence Q is a normal subgroup of the group G.

DEFINITION 9. Let G be a group. We form the sequence of subgroups $Q_1, \cdots, Q_i, \cdots$, where Q_1 is the commutator subgroup of G, while Q_{i+1} is the commutator subgroup of Q_i. All Q's are normal subgroups of the group G (see E)). If the above sequence contains the subgroup composed only of the identity of the group G, then the group G is called *solvable*.

The concepts of center and commutator play an important role in the theory of continuous groups.

EXAMPLE 8. Let G be the group of matrices given in Example 2. Let us denote by Z the aggregate of all the diagonal matrices of G which are such that each matrix has all its diagonal elements equal. It is easy to see that Z is a central normal subgroup of the group G. It can readily be shown that Z is the center of the group G. Let us denote by Q the normal subgroup of G composed of all the matrices with determinant unity (see Example 5). Since G/Q is evidently a commutative group (see Example 7), it follows that the commutator subgroup of G is contained in the group Q (see D)). It can be shown that Q is the commutator subgroup of the group G.

5. Intersection and Product of Subgroups. Direct Product

The concept of direct product plays an important part in the theory of groups: by decomposing a group into a direct product of other groups we reduce the study of the group to the consideration of simpler groups; on the other hand, by forming the product of given groups we have a method of constructing new groups.

We shall prove some properties of intersections and products of subgroups of a given group.

A) Let M be an aggregate of subgroups of G and let D be the intersection of all the subgroups in M; then D is a subgroup of the group G. If all the subgroups of M are normal subgroups of G, then D is also a normal subgroup of G.

In fact let a and b be elements of D. Let H be a subgroup in M; then $a \in H$ and $b \in H$ so that $ab^{-1} \in H$. Hence ab^{-1} belongs to an arbitrary subgroup of M, i.e., $ab^{-1} \in D$. Therefore, (see §2, B)) D is a subgroup of G. If all the elements of M are normal subgroups of the group G, then we have for an arbitrary $x \in G$, $x^{-1}ax \in H$, but since H is an arbitrary subgroup of M, it follows that $x^{-1}ax \in D$.

B) Let R be a subset of elements of a group G. We denote by M the set of all the subgroups of G which contain R. The intersection of all subgroups of the set M is the *minimal subgroup* of the group G which contains R. In the same way we define the *minimal normal subgroup* of the group G which contains R.

C) If H is a subgroup and N a normal subgroup of the group G, then the intersection $H \cap N = D$ of the groups H and N is a normal subgroup of the group H.

We have already shown (see A)) that D is a group and is therefore a sub-

group of H. Let $h \in H$ and $n \in D$; then $h^{-1}nh \in H$, since all the factors belong to H. But $h^{-1}nh \in N$ since $n \in N$ and N is a normal subgroup. Therefore $h^{-1}nh \in D$, and hence D is a normal subgroup of the group H.

D) Let H be a subgroup and N a normal subgroup of the group G. Then the product $HN = NH$ (see Definition 3) is a subgroup of the group G. In case H is a normal subgroup of G, HN is also a normal subgroup of G.

If a and b are elements of HN, then $a = hn$, $b = h'n'$, where h and h' belong to H, while n and n' belong to N. Therefore $ab^{-1} = hnn'^{-1}h'^{-1} = hh'^{-1}(h'nn'^{-1}h'^{-1})$, but since N is a normal subgroup, $h'nn'^{-1}h'^{-1} = n'' \in N$ and $ab^{-1} = (hh'^{-1})n'' \in HN$. Hence (see §2, B)) HN is a subgroup of the group G.

If H is a normal subgroup and $a = hn$, then for any $x \in G$ we have $x^{-1}ax = (x^{-1}hx)(x^{-1}nx) \in HN$, i.e., HN is a normal subgroup of the group G.

E) If $N_1, \cdots, N_k$ are normal subgroups of the group G, then it follows by induction from what we have shown in D) that $N_1 \cdots N_k$ is also a normal subgroup of the group G.

Theorem 2. *Let H be a subgroup and N a normal subgroup of the group G. Put $D = H \cap N$, and $P = HN$. Then the factor group H/D is isomorphic with the factor group P/N*

Proof. Let A be an element of H/D, then $A = Da$, where $a \in H$. Suppose $A' = Na$, where A' is an element of P/N. Since $D \subset N$, $A \subset A'$. Hence every element of H/D is contained in one and only one element of P/N. Now let $B' = bN = Nb$, where $b \in H$. Then $B = Db$ is an element of the group H/D and $B \subset B'$. Hence every element of the group P/N is contained in at least one element of the group H/D; we shall prove that it is contained in only one. Let A and B be two elements of H/D which are contained in the same element C' of P/N. We have $AB^{-1} \subset C'C'^{-1} = N$, moreover $AB^{-1} \subset H$, hence $AB^{-1} \subset D$, i.e., $A = B$. This establishes a one-to-one correspondence between the elements of the groups H/D and P/N.

Let us show that this correspondence between the elements of H/D and P/N is an isomorphism. Let A and B be two elements of H/D, A' and B' the corresponding elements of P/N, i.e., $A \subset A'$, $B \subset B'$. Then $AB \subset A'B'$, and hence to the element AB of the group H/D corresponds the element $A'B'$ of the group P/N, and we have an isomorphism between these groups.

We shall now take up a more special type of product of subgroups, namely the direct product.

Definition 10. Let H and K be two normal subgroups of the group G. We say the G is *decomposed into the direct product* of H and K if $HK = G$ and $H \cap K = \{e\}$.

F) We shall show that if G is decomposable into the direct product of H and K, then every element of H commutes with every element of K and every element of G can be represented uniquely in the form hk, where $h \in H$ and $k \in K$.

Let $h \varepsilon H$ and $k \varepsilon K$, and let us consider the commutator $hkh^{-1}k^{-1} = q$. Since K is a normal subgroup, $hkh^{-1} \varepsilon K$, and hence $q = (hkh^{-1})k^{-1} \varepsilon K$. On the other hand since H is a normal subgroup, $kh^{-1}k^{-1} \varepsilon H$, and $q = h(kh^{-1}k^{-1}) \varepsilon H$. Hence $q = e$, i.e., $hk = kh$.

Let $x \varepsilon G$. Since $G = HK$ it follows that $x = hk$, where $h \varepsilon H$, and $k \varepsilon K$. Suppose at the same time that $x = h'k'$, where $h' \varepsilon H$ and $k' \varepsilon K$. Then $hk = h'k'$. Multiplying this equation on the left by h^{-1} and on the right by k'^{-1}, we get $kk'^{-1} = h^{-1}h'$. But the left side of this equation belongs to K, while the right side belongs to H; hence $kk'^{-1} = h^{-1}h' = e$, i.e., $h = h'$, and $k = k'$.

In Definition 10 we started with a given group G. Let us now take the opposite point of view, and construct G from the groups H and K.

Definition 10′. Given two groups H and K, let us construct the set G of all pairs of elements (h, k), where $h \varepsilon H$, and $k \varepsilon K$. We define as the product of two pairs (h, k) and (h', k'), the pair (hh', kk'). Under this law of multiplication, G forms a group. The group G is called the *direct product* of the groups H and K.

It is obvious that the associative law holds in G, since it holds in the groups H and K. The identity of G is the pair (e, e'), where e is the identity of H, and e' is the identity of K. The element inverse to the pair (h, k) is the pair (h^{-1}, k^{-1}).

The two following propositions, G) and H), establish a connection between Definitions 10 and 10′.

G) Let G be decomposed into a direct product of normal subgroups H and K (see Definition 10). Denote by H' a group which is isomorphic with the group H, and by K' a group isomorphic with the group K, and let us form the direct product G' of the groups H' and K' (see Definition 10′). Then the group G' is isomorphic with the group G.

In fact let f be an isomorphic mapping of the group H' on the group H, and let g be an isomorphic mapping of the group K' on the group K. The isomorphic mapping h of the group G' on the group G is determined by the relation $h((h', k')) = f(h')g(k')$.

H) Let G be the direct product of H and K (see Definition 10′). Let us denote by H' the set of all elements of the group G which are of the form (h, e'), and by K' the set of all the elements of the group G which are of the form (e, k). Then H' and K' are normal subgroups of the group G, and G is decomposed into the direct product of H' and K', moreover H' is isomorphic with H, and K' is isomorphic with K.

Let us show that H' is a normal subgroup. If (h, e') and (h', e') are two elements of H', then $(h, e')(h', e')^{-1} = (hh'^{-1}, e') \varepsilon H'$ and therefore H' is a subgroup. If (a, b) is an arbitrary element of G, then $(a, b)^{-1}(h, e')(a, b) = (a^{-1}ha, e') \varepsilon H'$, and therefore H' is a normal subgroup. In the same way it can be proved that K' is a normal subgroup. The intersection of the groups H' and K' contains only the identity, since if $(h, e') = (e, k)$, then $h = e$,

$k = e'$. The product of the groups H' and K' coincides with G since every element $(h, k) \varepsilon G$ can be written in the form $(h, k) = (h, e')(e, k)$. Furthermore if we associate with every element $h \varepsilon H$ the element $(h, e) \varepsilon H'$, we obtain an isomorphism between the groups H and H'. In the same way we can establish the isomorphism of the groups K and K'.

I) Let G be decomposed into the direct product of normal subgroups H and K. Then the group H is isomorphic with the factor group G/K.

We can prove 1) by applying Theorem 2. In fact $H \cap K = \{e\}$ and $HK = G$, and therefore $H/\{e\}$ is isomorphic with G/K.

The definition of a direct product given here can be extended in a trivial way to the product of a finite number of factors. In what follows, however, we shall have to do with a countable number of factors and to avoid misunderstanding we pause here to discuss the matter.

Definition 10*. Let G be a group, and let M be a countable set of normal subgroups of G, $M = \{G_1, \cdots, G_n, \cdots\}$. We say that G is *decomposable* into the direct product of the subgroups of the set M, if the following conditions are fulfilled.

1) The minimal normal subgroup of the group G (see B)) which contains all the subgroups of the set M coincides with G.

2) If we denote by H_n the minimal normal subgroup of the group G (see B)) which contains all the subgroups of the set M with the exception of the subgroup G_n, then the intersection of all the subgroups H_n, $n=1, 2, \cdots$, contains only the identity e of the group G.

A*) The group G can be decomposed into the direct product of its two subgroups G_n and H_n (see Definitions 10* and 10).

The product G_nH_n is the normal subgroup of the group G (see D)) which, as can easily be seen, contains all the subgroups G_i. Therefore by condition 1) of Definition 10*, $G_nH_n = G$. Denote by G'_n the intersection of all the groups H_k, $k=1, 2, \cdots$, with the exception only of the group H_n. It is obvious that $G_n \subset G'_n$. From condition 2) of Definition 10* it follows that the intersection $G'_n \cap H_n = \{e\}$. Hence the intersection $G_n \cap H_n = \{e\}$, and G can be decomposed into the direct product of the groups G_n and H_n.

B*) For $i \neq j$ every element of the group G_i commutes with every element of the group G_j. Furthermore, every element $x \varepsilon G$ can be uniquely represented as a product $x = x_1 \cdots x_n$ where $x_i \varepsilon G_i$, $i = 1, 2, \cdots, n$, and n is a sufficiently large number depending on x.

Since $G_i \subset H_j$, the commutativity of the elements of the groups G_i and G_j follows from A*) (see F)). We remark further that the set G' of all products of the form $x = x_1 \cdots x_n$, where $x_i \subset G_i$, $i = 1, \cdots, n$, $n = 1, 2, \cdots$, is a normal subgroup of the group G, and every group G_k belongs to G'. In this way it follows from condition 1) of Definition 10* that $G' = G$ and therefore every element $x \varepsilon G$ can be written in the form of the product given above. The uniqueness of such a decomposition into a product follows easily from F) and A*).

Definition 10*′. Let M be a countable aggregate of groups $M = \{G_1, \cdots, G_n, \cdots\}$. We shall construct a new group G from the groups of the set M, which we call the *direct product* of the groups of the set M. The elements of G will be the sequences $x = \{x_1, \cdots, x_n, \cdots\}$, where $x_n \varepsilon G_n$, $n = 1, 2, \cdots$, and only a finite number of the x_n are not identities. The product of two sequences x and $y = \{y_1, \cdots, y_n, \cdots\}$ is defined as the sequence

$$xy = \{x_1y_1, \cdots, x_ny_n, \cdots\}.$$

It is not hard to see that the group G obtained in this way does not depend on the way in which the groups of the set M are numbered. The identity of G is $e = \{e_1, \cdots, e_n, \cdots\}$, where e_n is the identity of the group G_n, $n = 1, 2, \cdots$. The inverse of the element x is the element $x^{-1} = \{x_1^{-1}, \cdots, x_n^{-1}, \cdots\}$. It is easy to see that all the group axioms hold in the set G.

The equivalence of Definitions 10* and 10*′ is established without difficulty in the same way as was done above for Definitions 10 and 10′ (see G) and H)). Because of the triviality of these generalizations, we shall not stop here to consider them.

Example 9. Let G be a countable commutative group all of whose elements, with the obvious exception of the identity, are of prime order ρ. It is not hard to show that the group G can be decomposed into the direct product of a countable number of cyclic subgroups of order ρ, i.e., subgroups of the form $H = \{e, a, a^2, \cdots, a^{\rho-1}\}$, where $a^\rho = e$.

Example 10. Let G be the group of matrices given in Example 2. The totality G' of all matrices with a positive determinant forms a subgroup of the group G. Let us decompose G' into a direct product.

Let us denote by Z the totality of all diagonal matrices of G' which are such that the diagonal elements of each matrix are equal and positive. We denote by Q the totality of all matrices whose determinant is unity. It is easy to see that Z and Q are normal subgroups of G and that G' is decomposed into the direct product of Z and Q. In fact, the intersection of Z and Q contains only the unit matrix, while every matrix of G' can be represented as the product of a matrix Z by a matrix Q.

6. Commutative Groups

In this section we give a proof of the fundamental theorem of commutative groups (see F)). We shall use this result in Chapter 5 only, and it is not essential to an understanding of the other parts of this book.

We consider here commutative groups only, and we shall use the additive notation.

A) A finite system of elements $g_1, g_2, \cdots, g_k$ of the group G is called *linearly independent* if the equation

$$a_1g_1 + \cdots + a_kg_k = 0,$$

where $a_1, \cdots, a_k$ are integers, implies that

$$a_1 = 0, \cdots, a_k = 0.$$

An infinite system of elements of the group G is called *linearly independent* if all its finite subsystems are linearly independent. The maximal number of linearly independent elements of G is called the *rank* of G. It is obvious that a linearly independent system cannot contain elements of finite order.

B) A finite or infinite system

$$g_1, \cdots, g_n, \cdots \tag{1}$$

of elements of a group G is called a system of *generators* of this group if every element $g \in G$ can be written in the form

$$g = a_1g_1 + \cdots + a_kg_k, \tag{2}$$

where $a_1, \cdots, a_k$ are integers. If the system (1) of generators of the group G is linearly independent, then the representation (2) of every element g is, as can easily be seen, unique.

C) Let G be a group having a finite system

$$g_1, \cdots, g_k \tag{3}$$

of linearly independent generators. Then every subgroup H of the group G also contains a finite system of linearly independent generators, whose number does not exceed k.

The proof is by induction. For $k = 0$ the statement is obvious, as in this case G contains only zero, and H coincides with G. Suppose that the proposition is proved for $k = m$; we shall then prove it for $k = m + 1$. Let $k = m + 1$, and let us designate by G' the subgroup of the group G with the generators $g_1, \cdots, g_m$, and by H' the intersection of H and G', $H' = H \cap G'$. From the hypothesis of the induction the subgroup H' of the group G' has a finite system of linearly independent generators

$$h_1, \cdots, h_n \tag{4}$$

with $n \leq m$. Now let

$$h = a_1g_1 + \cdots + a_mg_m + a_{m+1}g_{m+1}$$

be an arbitrary element of the group H'. Because of the condition of linear independence, the number a_{m+1} is uniquely determined by the element h. If for every choice of the element h, the number a_{m+1} is equal to zero, then $H \subset G'$, i.e., $H = H'$ and hence H has a system of linearly independent generators (4). Suppose that for some elements $h \in H$, the number a_{m+1} is different from zero. Then there exist elements h for which the number a_{m+1} is positive, since for every element h of the group H there is an element $-h$. Let us denote by h_{n+1} the element for which the number a_{m+1} achieves its least positive value a'_{m+1},

$$h_{n+1} = a_1'g_1 + \cdots + a_m'g_m + a_{m+1}'g_{m+1}.$$

We shall show that for every $h \varepsilon H$ the number a_{m+1} is divisible by a_{m+1}'. We write the number a_{m+1} in the form $a_{m+1} = b_{n+1}a_{m+1}' + r$, where b_{n+1} and r are integers and $0 \leqq r < a_{m+1}'$. Then

$$h - b_{n+1}h_{n+1} = (a_1 - b_{n+1}a_1')g_1 + \cdots + (a_m - b_{n+1}a_m')g_m + rg_{m+1}$$

is an element of the group H for which a_{m+1} has the value r. Since $0 \leqq r < a_{m+1}'$, and a_{m+1}' is the least positive value of the number a_{m+1}, we have $r = 0$. Hence a_{m+1} is divisible by a_{m+1}' and the element $h - b_{n+1}h_{n+1}$ belongs to G', i.e. belongs to H', and we have

$$h - b_{n+1}h_{n+1} = b_1h_1 + \cdots + b_nh_n$$

(see (4)), and therefore

$$h = b_1h_1 + \cdots + b_nh_n + b_{n+1}h_{n+1}.$$

Hence the system $h_1, \cdots, h_n, h_{n+1}$ is a system of generators of the subgroup H. The linear independence of this system follows from the linear independence of the system (4) and the definition of the element h_{n+1}.

The following proposition D) forms a basis for the proof of theorem F).

D) Let $a = \|a_{ij}\|$ be a matrix with p rows, q columns, and integer elements. Then there exist two *unimodular matrices* (i.e., square matrices whose elements are integers and whose determinants are ± 1) s and t of order p and q respectively which are such that the matrix $b = \|b_{ij}\| = sat$ (see Example 2) has a so-called *canonical form*, i.e., it satisfies the following conditions: a) for $i \neq j$, $b_{ij} = 0$, b) the number $b_{i+1,i+1}$ is divisible by the number b_{ii}, c) the numbers b_{ii} are non-negative.

To prove this we introduce the so-called *elementary operations* on a matrix x with integer elements. Operation 1 consists in multiplying any row of the matrix x by -1, operation 2 consists in an interchange of any two rows of the matrix x, operation 3 consists in the addition to any row of the matrix x of an integer multiple of some other row. Analogously, we define operations 1′, 2′, and 3′ as applied to columns rather than rows of the matrix x. It is easy to see that each one of the operations 1, 2, or 3 can be effected by multiplying the matrix x on the left by a unimodular matrix. Analogously, each one of the operations 1′, 2′, and 3′ can be effected by multiplying the matrix x on the right by a unimodular matrix. In this way to prove D) it is sufficient to show that the matrix x can be reduced to the canonical form by means of successive applications of the elementary operations.

We shall show that if in the matrix $x = \|x_{ij}\|$ the element x_{11} divides all the elements of the first row and column, then by successive application to x of a series of elementary operations the matrix x can be transformed into a matrix $y = \|y_{ij}\|$ which is such that $y_{11} = x_{11}$, and all the other elements of the first row and the first column of y are equal to zero.

Since x_{i1} is divisible by x_{11}, we may write $x_{i1} = -rx_{11}$, where r is an integer. Adding to the i-th row of the matrix x the first row multiplied by r we get a new matrix which has a zero in the i-th place of the first column. Applying this operation to every row, beginning with the second, and then to every column, beginning with the second, we obtain the desired result.

Let us denote for brevity by (x) the minimum of the positive absolute values of the elements of x, and show that if it is false that every element of the matrix x is divisible by (x), then the matrix x can be transformed by means of elementary operations into a matrix y which is such that $(y) < (x)$.

It is easy to see that by means of an interchange of rows, and of columns, and also by changing sign in some row, the matrix x can be reduced to a matrix which satisfies the condition $(x) = x_{11}$. If now the first column of the matrix x contains an element x_{i1} which is not divisible by x_{11}, then we shall have $x_{i1} = -rx_{11} + n$, where $0 < n < x_{11}$. Adding to the i-th row of the matrix x its first row multiplied by r, we shall get a new matrix y for which $(y) \leqq n < (x)$. If now x_{11} divides all the elements of the first column, but not all the elements of the first row, we can apply a similar operation and obtain a matrix y which satisfies the condition $(y) < (x)$. If, however, all the elements of the first row and the first column are divisible by x_{11}, this matrix can be reduced to the form in which the only element different from zero in the first row and column is the element x_{11}. If the resulting matrix contains an element x_{ij} which is not divisible by x_{11}, we add the i-th row to the first row and obtain a matrix not all of whose elements in the first row are divisible by x_{11}, i.e., a matrix to which can we can again apply the reasoning above.

It follows from what we have just proved that by means of elementary operations the matrix x can be transformed into a matrix z all of whose elements are divisible by (z). In fact, if not every element of the matrix x is divisible by (x) then, as we have just shown, the matrix x can be transformed into a matrix y with $(y) < (x)$. Since we are dealing here with whole numbers only (x) can be diminished in this way only a finite number of times, and therefore after a finite number of steps our process will terminate by reducing the matrix to the desired form.

Hence by means of applications of elementary operations it is possible to reduce the matrix x to a form in which all of its elements are divisible by (x). Moreover, also by means of elementary operations, it is possible to get $x_{11} = (x)$ and all other elements of the first row and column equal to zero, without destroying the divisibility of the elements of x by (x). The matrix thus obtained is said to be in *semi-canonical* form. Let us denote by x' the matrix obtained from the matrix x by crossing out the first row and column. Every element of x' is divisible by x_{11}. Reducing the matrix x' to a semi-canonical form, and repeating the process we shall finally reduce the matrix x to the canonical form.

In this way, the proof of D) is completed.

E) Let X be a group having a system of linearly independent generators, and

let Y be a subgroup. Then we can select in X a system $x_1', \cdots, x_q'$ of linearly independent generators which are such that the elements

$$d_1 x_1', \cdots, d_r x_r', \qquad r \leqq q,$$

form a system of generators of the group Y where $d_i > 0$, $i = 1, 2, \cdots, r$, and d_{i+1} is divisible by d_i, $i = 1, \cdots, r - 1$.

Let

$$x_1, \cdots, x_q \tag{5}$$

be a system of linearly independent generators of the group X, and

$$y_1, \cdots, y_p \tag{6}$$

be an arbitrary system of linearly independent generators of the group Y (see C)). Then we shall have the following relations,

$$y_i = a_{i1} x_1 + \cdots + a_{iq} x_q, \qquad i = 1, \cdots, p, \tag{7}$$

where $\|a_{ij}\| = a$ is a matrix with integral elements. Let us further denote by $s = \|s_{ki}\|$ and $t = \|t_{jl}\|$ two unimodular matrices of orders p and q respectively. Making use of these matrices we introduce into the groups X and Y new systems of generators

$$x_1', \cdots, x_q' \tag{8}$$

and

$$y_1', \cdots, y_p' \tag{9}$$

by means of the relations

$$x_j = t_{j1} x_1' + \cdots + t_{jq} x_q', \qquad j = 1, 2, \cdots, q, \tag{10}$$

$$y_k' = s_{k1} y_1 + \cdots + s_{kp} y_p, \qquad k = 1, \cdots, p. \tag{11}$$

It is permissible to introduce new systems of generators in the groups X and Y by means of these relations because the matrices t and s have unimodular determinants, so that relations (10) and (11) can be solved for the elements (8) and (6); hence these elements can be expressed in terms of linear forms of the elements of (5) and (7) with integral coefficients. For the new system of generators we get instead of (7), the following relation:

$$y_k' = \sum_{i=1}^{p} \sum_{j=1}^{q} \sum_{l=1}^{q} s_{ki} a_{ij} t_{jl} x_l' = a_{k1}' x_1' + \cdots + a_{kq}' x_q', \qquad k = 1, \cdots, p,$$

where $\|a_{kl}'\| = a'$ is a matrix with integer elements, and $a' = sat$. Choosing the matrices s and t in such a way that the matrix a' has a canonical form

(see D)), we arrive at a new system of generators $x_1', \cdots, x_q'$ of the group G which satisfies the assertion E).

F) A group G having a finite system of generators is decomposable into the direct sum of cyclic subgroups

$$U_1, \cdots, U_m; \qquad V_1, \cdots, V_n,$$

where U_i, $i = 1, \cdots, m$, is a free cyclic group and V_j, $j = 1, \cdots, n$, is a cyclic group of finite order $\tau_j > 1$ with τ_{j+1} divisible by τ_j, $j = 1, \cdots, n - 1$ (see §2, B)). In case G has a finite system of linearly independent generators, then G has no summands of finite order.

Let $g_1, \cdots, g_q$ be a finite system of generators of the group G. Let us denote by X the set of all linear forms of the type

$$x = a_1x_1 + \cdots + a_qx_q \tag{12}$$

with integral coefficients $a_1, \cdots, a_q$ and variables $x_1, \cdots, x_q$. We can define naturally in X an operation of addition, so that X becomes a group having a system $x_1, \cdots, x_q$ of linearly independent generators. With every element $x \in X$ (see (12)) we associate the element $f(x) = a_1g_1 + \cdots + a_qg_q$ of the group G. The mapping f is obviously a homomorphism of the group X on the group G. The kernel of the homomorphism f we denote by Y. Let us now choose in X the system

$$x_1', \cdots, x_q' \tag{13}$$

of linearly independent generators which was constructed in E). Suppose that $g_i' = f(x_i')$, $i = 1, \cdots, q$. Then $g_1', \cdots, g_q'$ is a system of generators of the group G. These generators satisfy the following relations:

$$d_1g_1' = 0, \cdots, d_rg_r' = 0$$

(see E)). On the other hand if the relation

$$b_1g_1' + \cdots + b_qg_q' = 0$$

holds, then b_i is divisible by d_i for $i = 1, \cdots, r$ and is equal to zero for $i = r + 1, \cdots, q$. In fact suppose that

$$x' = b_1x_1' + \cdots + b_qx_q';$$

then $f(x') = 0$ and hence $x' \in Y$, i.e., the numbers $b_1, \cdots, b_q$ satisfy the above relations since the system of generators (13) is linearly independent, and $d_1x_1', \cdots, d_rx_r'$ form a system of generators of the group Y. Let now $d_1, \cdots, d_s$ be those numbers of the system $d_1, \cdots, d_r$ which are equal to unity. Let us denote the numbers $d_{s+1}, \cdots, d_r$ by $\tau_1, \cdots, \tau_n$. Further suppose that $g_{s+j}' = v_j$, $j = 1, \cdots, n$, $g_{r+i}' = u_i$, $i = 1, \cdots, q - r = m$. The subgroup of the group G with the generator u_i we denote by U_i, and the subgroup with the

generator v_j we denote by V_j. It is easy to see that the subgroups constructed in this way give a decomposition of the group G into a direct sum.

If G has a finite system of linearly independent generators, then each of its subgroups has the same property (see C)), and therefore G has no elements of finite order. In this case the decomposition into a direct sum contains no summands of finite order.

Hence the proposition F) is completely proved.

In conclusion we remark that the decomposition of G into a direct sum which we have obtained is unique up to an isomorphism, which means that the number m and the system $\tau_1, \cdots, \tau_n$ are invariants of the group G. The uniqueness of decomposition will, however, not be used by us in the future, and therefore I shall leave this fact without proof.

CHAPTER II

TOPOLOGICAL SPACES

Just as the theory of groups studies the algebraic operation of multiplication in its purest aspect, so abstract topology sets as its goal the investigation of the operation of passing to the limit, disregarding all other properties of the elements under consideration. If a group can be regarded as a generalization of the concept of real numbers, then a topological space should also be treated as a generalization of these same real numbers. Only in the first case the operation of multiplication is generalized, while in the second it is the limiting operation, or, what is the same, the concept of limit point which is generalized.

Given a set M of real numbers it is possible to ascertain of any real number whether it is or is not a limit point of the set M. It is possible to formulate in terms of limit points the condition for convergence of a sequence of real numbers, and in general all concepts connected with passing to a limit. The concept of a limit point is at the foundation of the structure of a topological space. It seems more practical, however, to axiomatize not the concept of limit point, but the entirely equivalent concept of closure. Adding to a given set M all its limit points we get the so-called closure $\overline{M}$ of the set M. $\overline{M}$ consists of all the numbers which belong to M, together with the limits of the numbers of M. Hence, knowing what a limit point is, we also know what closure is. Conversely, it is possible to formulate the concept of a limit point in terms of closure. If the point a does not belong to the set M, then it is a limit point of M if and only if $a \varepsilon \overline{M}$. However, in case $a \varepsilon M$, this criterion is insufficient, since a can be an isolated point of the set M. But if a belongs to M and is at the same time a limit point of M, then a is a limit point of $M - a$, i.e., $a \varepsilon \overline{M - a}$; this condition is sufficient, moreover it is applicable also when a does not belong to M, since in that case $M = M - a$. Hence it follows that a is a limit point of M if and only if $a \varepsilon \overline{M - a}$.

7. The Concept of a Topological Space

Axiomatizing the concept of closure, we arrive at the concept of topological space.

Definition 11. A set R of arbitrary elements is called a *topological space* if:

1) To every set M of elements of the space R there corresponds a set $\overline{M}$ which is called the *closure* of M.

2) If M contains only one element a, then $\overline{M} = M$, or what is the same, $\bar{a} = a$.

3) If M and N are two sets of elements of the space R, then $\overline{M \cup N} = \overline{M} \cup \overline{N}$, i.e. the closure of the sum of two sets is equal to the sum of the closures.

4) $\overline{\overline{M}} = \overline{M}$, i.e., the operation of closure applied twice gives the same result as a single application of the operation.

The elements of a topological space are called *points*. A point a of the space R is called a *limit point* of the set M of elements of R if $a \in \overline{M - a}$.

A) Let us show that $M \subset \overline{M}$.

In fact, let $a \in M$, then $M = M \cup a$. Taking the closure of both sides of this equation we get $\overline{M} = \overline{M \cup a} = \overline{M} \cup \bar{a} = \overline{M} \cup a$, that is $a \in \overline{M}$, and $M \subset \overline{M}$.

B) If $M \subset N$, then $\overline{M} \subset \overline{N}$.

In fact, $N = M \cup N$. Taking the closure of both sides of this equation we get $\overline{N} = \overline{M} \cup \overline{N}$, i.e., $\overline{M} \subset \overline{N}$.

Definition 12. A set F of elements of a topological space R is called *closed* if $\overline{F} = F$. A set G of elements of a topological space R is called *open* if $R - G$ is a closed set.

As can be seen from Definition 12 closed sets and open sets are complements of one another in the space R. Therefore to every statement concerning closed sets corresponds some statement concerning open sets. We shall take this remark into consideration in the proofs of some simple theorems which follow.

C) The sum of a finite number of closed sets is a closed set.

In fact if E and F are two closed sets, then $\overline{E \cup F} = \overline{E} \cup \overline{F} = E \cup F$, $E \cup F$ is closed. By induction this assertion can be extended to any finite number of summands.

The corresponding proposition for open sets is the following:

D) The intersection of any finite number of open sets is an open set.

The proof of this proposition is quite trivial, and in the future similar proofs will be omitted, but it is worth while to carry out the proof once. Let G and H be two open sets of R. Then $E = R - G$ and $F = R - H$ are closed sets. The intersection $G \cap H$ is the complement of $E \cup F$, i.e., $G \cap H = R - (E \cup F)$. But $E \cup F$ is a closed set (see C)), and hence $G \cap H$ is an open set.

E) Let Σ be a system of closed sets of the space R, and let D be the intersection of all the sets contained in Σ. Then D is a closed set.

In fact, let F be a set of the system Σ. Then $D \subset F$, and hence $\overline{D} \subset \overline{F} = F$. Since F is an arbitrary set of the system Σ, $\overline{D} \subset D$. But $\overline{D} \supset D$ (see A)), hence $\overline{D} = D$.

The corresponding proposition for open sets is the following:

F) The sum of an arbitrary number of open sets is an open set.

G) We remark that, except for the trivial case in which the space R contains only a single point every space R contains two closed sets: R itself, and the null set. Therefore in every set R there are also two open sets, the set R and the null set.

In fact, the closure of every subset of R is in R, and therefore $\overline{R} \subset R$, and from this together with A) it follows that $\overline{R} = R$, i.e., R is closed. Further if R contains two distinct points a and b, then the null set, being the intersection of the two sets each containing the one point a or b is closed (see E)).

Example 11. Let R be an infinite set. Let us define in R the operation of closure by means of the following conditions. If M is a finite subset of R, we shall suppose that $\overline{M} = M$. If M is an infinite subset of R we shall sup-

pose that $\overline{M} = R$. It is easy to check that the operation of closure which we have just defined satisfies the conditions of Definition 11.

EXAMPLE 12. Let R be a set. We shall define in R the operation of closure by supposing that $\overline{M} = M$ for every subset M of R. It is easy to see that by this operation R becomes a topological space, since, as can easily be verified, conditions 2, 3, and 4 of Definition 11 are satisfied. Every subset of the space R is closed. A space R defined in this way we shall call *discrete*.

8. Neighborhoods

In this section we shall give a method of defining a topological space by means of neighborhoods rather than by means of the operation of closure. This method is rather important and is often used as the foundation of the axiomatic treatment of the concept of a topological space.

According to Definition 11, in order to determine a topological space R, it is necessary to associate with each subset M of R its closure $\overline{M}$. It can be seen, however, that it is not necessary to give the closure of every set but it is sufficient to specify the family of all the closed sets in order to determine the closure of every set of R uniquely. The justification of this statement can be found in the following proposition.

A) Let M be some set of R and let Σ be the totality of all the closed sets of R which contain M. If we denote by D the intersection of all the sets of Σ, then $\overline{M} = D$. In other words $\overline{M}$ is the minimal closed set containing M.

Since $\overline{\overline{M}} = \overline{M}$, it follows that $\overline{M}$ is a closed set. Moreover $\overline{M} \supset M$ and hence $\overline{M} \subset \Sigma$, that is $D \subset \overline{M}$. Furthermore $D \supset M$, but since D is the intersection of closed sets, $D = \overline{D} \supset \overline{M}$. Hence $D = \overline{M}$.

In order to give all the closed sets of the space R it is sufficient to give all the open sets of the space R, since every closed set is the complement of some open set, and the complement of every open set is a closed set. Hence in order to determine the topological space R it is sufficient to give all the open sets of R. Making use of the fact that the sum of an arbitrary number of open sets is also an open set we arrive at the following simplification.

DEFINITION 13. A system Σ of open sets of a space R is called a *basis* of R if every open set of R can be obtained as a sum of open sets belonging to Σ. A basis Σ of a space R is also called a *complete system of neighborhoods* of the space R, while every open set of the system Σ is a *neighborhood* of every point contained in this open set.

The simplest example of a basis of a space R is the totality of all the open sets of R.

Knowing a basis of the space R we thereby know all the open sets of R and therefore closure is uniquely determined in R. Hence in order to determine a space R it is sufficient to specify one of its bases.

As is seen from Definition 13 the concept of neighborhood is not completely determined by the operation of closure in R, but it also depends on the choice

of the basis Σ. Therefore, when speaking of neighborhoods in the future we shall keep in mind that some definite basis Σ has been chosen.

B) In order that a system of neighborhoods Σ form a basis of the space R it is necessary and sufficient that for every open set G and element a belonging to G, there exist an open set U of the system Σ such that $a \varepsilon U \subset G$.

If Σ is a basis of R, then there exists a system Σ' of open sets of Σ such that G is the sum of all the open sets of Σ'. Then there exists an open set $U \varepsilon \Sigma'$ such that $a \varepsilon U$. Since G is a sum of open sets among which is U, it follows that $U \subset G$.

Let us now suppose that the condition formulated above is satisfied for Σ, and let G be an arbitrary open set of R. Then for every $x \varepsilon G$, there can be found an open set $U_x \varepsilon \Sigma$, which is such that $x \varepsilon U_x \subset G$. The sum of all the open sets U_x with an arbitrary $x \varepsilon G$ is obviously equal to G, and hence Σ is a basis of the space R.

By analogy with the criterion B) we give the following definition.

B′) A system Σ' of neighborhoods of a point a is called a *basis about the point* a or a *complete system of neighborhoods of the point* a if for every open set G containing the point a a neighborhood $U \varepsilon \Sigma'$ can be found such that $U \subset G$. It follows directly from B) that if Σ is a basis of the whole space, then the totality of the open sets of the system Σ which contain the point a forms a basis about the point a.

As we have remarked above, the knowledge of a complete system of neighborhoods Σ in the space R enables one to determine uniquely the operation of closure in this space. We shall show concretely how the above transition from neighborhoods to the operation of closure can be accomplished.

C) Let a be a point, and M a set of R. Then a belongs to $\overline{M}$ if and only if every neighborhood U of the point a contains a point belonging to M. By a neighborhood of the point a, we understand here any element of a basis about the point a (see B′)).

For suppose that a does not belong to $\overline{M}$. Then $R - \overline{M}$ is an open set containing a, and hence there exists an open set $U \varepsilon \Sigma'$ such that $a \varepsilon U \subset R - \overline{M}$ (see B′)). Hence there exists a neighborhood U of the point a which does not intersect M. If further V is a neighborhood of the point a which does not intersect M, then $M \subset R - V = F$, where F is a closed set since V is an open set. Then $\overline{M} \subset \overline{F} = F$, i.e., $\overline{M}$ does not contain a. Hence in order that $\overline{M}$ should not contain a, it is necessary and sufficient that a should have a neighborhood which does not intersect M. But this assertion is equivalent to C).

D) If Σ is a complete system of neighborhoods of a topological space R (see Definition 13), then the following conditions are fulfilled:

a) If a and b are two distinct points of the space R, then a neighborhood $U \varepsilon \Sigma$ of the point a can be found which does not contain the point b.

b) If $U \varepsilon \Sigma$ and $V \varepsilon \Sigma$ are two neighborhoods of the point $a \varepsilon R$, then a neighborhood $W \varepsilon \Sigma$ of the same point a can be found such that $W \subset U \cap V$.

To prove condition a) we observe that $R - b$ is an open set, and hence

from B) there exists a neighborhood U of the point a which is contained in $R - b$. To prove condition b) we apply the same remark B) to the open set $U \cap V$, which contains the point a.

Conditions a) and b) are important inasmuch as they in turn can be taken as axioms for neighborhoods in a topological space. In greater detail this thought is expressed in Theorem 3, which is at the same time a converse of the propositions C) and D) taken together.

THEOREM 3. *Let R be a set, and let Σ be a system of its subsets for which the following conditions are satisfied:*

a) *For any two distinct points a and b of R there exists a set U of the system Σ which is such that $a \varepsilon U$, but $b \notin U$.*

b) *For any two sets U and V of the system Σ which contain the point $a \varepsilon R$, there exists a set W of the system which is such that $a \varepsilon W \subset U \cap V$.*

We shall now define in R the operation of closure of an arbitrary set $M \subset R$, by stating that $a \varepsilon \overline{M}$ if and only if every subset of the system Σ which contains a intersects M. The operation of closure thus defined satisfies Definition 11, *and hence R is a topological space. Moreover the system Σ is a complete system of neighborhoods of the space R.*

PROOF. Condition 1) of Definition 11 is satisfied in R, since the operation of closure is defined. We now proceed to show that conditions 2), 3), and 4) are also satisfied. We shall call the set $U \varepsilon \Sigma$ a neighborhood of the point $a \varepsilon R$ if $a \varepsilon U$.

Let M contain only a single point a. Since every neighborhood of the point a contains a, then $a \varepsilon \overline{M}$. Let b be a point of R distinct from a. By condition a) of the theorem there exists a neighborhood U of the point b which does not contain a. Hence b does not belong to $\overline{M}$, and $\overline{M} = a$, so that condition 2) of Definition 11 is satisfied.

Let M and N be two subsets of R. If $a \varepsilon \overline{M} \cup \overline{N}$, then every neighborhood U of the point a intersects either M or N, but in that case U intersects $M \cup N$, i.e., $a \varepsilon \overline{M \cup N}$. If now a does not belong to $\overline{M} \cup \overline{N}$, there exist neighborhoods U and V of the point a which are such that U, V do not intersect M and N respectively. By condition b) of the theorem there exists a neighborhood W of the point a which is contained in $U \cap V$. W does not intersect $M \cup N$, and hence a does not belong to $\overline{M \cup N}$. Hence $\overline{M \cup N} = \overline{M} \cup \overline{N}$, and condition 3) of Definition 11 is satisfied.

Before taking up the proof that condition 4) of Definition 11 is satisfied, we remark that under the operation of closure introduced in Theorem 3, $N \subset \overline{N}$. In fact, if $x \varepsilon N$, then every neighborhood of x intersects N, since it contains x. Hence $x \varepsilon \overline{N}$, i.e., $N \subset \overline{N}$.

Let $a \varepsilon \overline{\overline{M}}$. This implies that every neighborhood U of the point a intersects $\overline{M}$, i.e. there exists a point b, which is such that $b \varepsilon U$ and $b \varepsilon \overline{M}$. But then U is a neighborhood of the point b, and since $b \varepsilon \overline{M}$, it follows that U

intersects M. In this way, an arbitrary neighborhood U of the point a intersects M, i.e., $a \in \overline{M}$ and hence $\overline{\overline{M}} \subset \overline{M}$. On the other hand we have shown above that $\overline{M} \subset \overline{\overline{M}}$. Hence $\overline{\overline{M}} = \overline{M}$, i.e., condition 4) of Definition 11 is satisfied.

We shall now show that Σ is a complete system of neighborhoods of the space R. Let us show first of all that every set $U \in \Sigma$ is an open set of the space R. To do this, it is sufficient to prove that $F = R - U$ is closed. If the point x does not belong to F, then $x \in U$, and hence the neighborhood U of the point x does not intersect F. Hence x does not belong to $\overline{F}$. Therefore $\overline{F} = F$, and hence U is an open set. If now G is an arbitrary open set of R, and $a \in G$, then $R - G = E$ is closed and does not contain a. Hence there exists a neighborhood W of the point a which does not intersect E. In this way for an arbitrary open set G and point $a \in G$, there exists a neighborhood W which is such that $a \in W \subset G$, i.e., Σ is a basis of R (see B)).

Hence the proof of Theorem 3 is complete.

E) Theorem 3 enables us to define a topological space R by means of a system Σ of subsets of the space R which satisfies conditions a) and b) of Theorem 3 rather than by means of the operation of closure. Given the system Σ, the operation of closure in R is determined by the method given in Theorem 3, and this system Σ is called the *defining system of neighborhoods* of the space R.

If the space R is given by means of a defining system of neighborhoods, then the operation of closure in R is uniquely determined. The converse is not true, however. If R is given by means of the operation of closure then the defining system of neighborhoods is not uniquely determined. Therefore, the question arises under what conditions two different systems of defining neighborhoods of the same set R lead to the same operation of closure.

F) Two defining systems of neighborhoods Σ and Σ' are called *equivalent* if they lead to the same operation of closure in R. In order that two systems Σ and Σ' of defining neighborhoods be equivalent, it is necessary and sufficient that for every point a and neighborhood $U \in \Sigma$ of the point a there can be found a neighborhood $U' \in \Sigma'$ of the point a such that $U' \subset U$, and conversely, for every neighborhood $V' \in \Sigma'$ of the point a there can be found a neighborhood $V \in \Sigma$ of the same point such that $V \subset V'$.

The necessity of this condition is obvious. In fact, since U is an open set containing a, and Σ' is a basis of R, there exists a $U' \in \Sigma'$ such that $a \in U' \subset U$. In the same way we can prove the existence of V for a given V'. Supposing now that the conditions of equivalence of Σ and Σ' are satisfied, we shall show that Σ and Σ' lead to the same operation of closure. Suppose that $a \in \overline{M}$, where the closure is constructed with respect to the system Σ. Let V' be an arbitrary neighborhood of the point a in the system Σ'. From the condition of equivalence there exists a neighborhood $V \in \Sigma$ of the point a such that $V \subset V'$, but V intersects M, and therefore V' intersects M. Since V' is an arbitrary neighborhood of the point a in the system Σ', it follows that $a \in \overline{M}$, where the operation of closure is defined with respect to the system Σ'.

We now formulate in terms of neighborhoods a necessary and sufficient con-

dition that a subset G of the space R be an open set. This condition is as follows:

G) The subset G of a space R is an open set if and only if for every point $a \varepsilon G$ there exists a neighborhood U of the point a which is contained in G.

The necessity of this condition follows directly from the fact that the defining system of neighborhoods is a basis of the space R. If now G satisfies the above condition, we shall prove that $R - G = F$ is a closed set. Suppose that a does not belong to F. Then $a \varepsilon G$, and hence there exists a neighborhood U of the point a which does not intersect F. Hence a does not belong to $\overline{F}$, and F is, therefore, closed.

We now give in terms of neighborhoods a necessary and sufficient condition for a point a to be a limit point of a set M. This condition can be formulated as follows:

H) In order that a point a be a limit point of a set M, it is necessary that every neighborhood of the point a contain infinitely many points of M, and it is sufficient that every neighborhood of the point a contain at least one point of M distinct from a.

In fact, suppose that $a \varepsilon \overline{M - a}$, and that some neighborhood U of the point a contains only a finite set N of points of the set $M - a$. Then $U - N$ is an open set containing a, and hence there exists a neighborhood V of the point a which is contained in $U - N$, i.e., a neighborhood V which does not intersect the set $M - a$; but this is impossible, since $a \varepsilon \overline{M - a}$. If conversely, every neighborhood of the point a contains a point of M distinct from a, this means that every neighborhood of the point a intersects $M - a$, i.e., $a \varepsilon \overline{M - a}$, and hence a is a limit point of M.

EXAMPLE 13. Let R^n be the n-dimensional Euclidean space. Every point of R^n is determined by its n cartesian coordinates. We consider the sequence of points x_k, $k = 1, 2, \cdots$. The coordinates of the point x_k we denote by x_k^i, $i = 1, \cdots, n$. We say that the sequence x_k converges to the point x with coordinates x^i, if $\lim_{k\to\infty} x_k^i = x^i$ for every i. Let M be a set of points of R^n. We say that x is a limit point of the set M if there exists in M a sequence of points distinct from x which converges to x. We define as the *closure* $\overline{M}$ of the set M the totality of the points which either belong to M or are limit points of M. It follows readily that the operation of closure thus defined satisfies all the conditions of Definition 11. Hence R^n becomes a topological space.

Since R^n is a Euclidean space, in it is defined the distance between any two points. The set of all points of R^n whose distance from a fixed point a is less than a given number r is called the *sphere* with center a and radius r. It is easily seen that every sphere is an open set in R^n. It can also be shown that the aggregate of all spheres forms a basis of R^n. Similarly, the aggregate of all spheres with rational centers and rational radii forms a basis of R^n.

EXAMPLE 14. In this section we have given a method of defining the operation of closure by means of neighborhoods. Another rather important way of defining the same operation is by means of a metric. It is not possible, how-

ever, to define the operation of closure in all topological spaces by means of a metric. Therefore the important class of metrizable topological spaces is singled out.

The set R of elements is called a *metric space* if to every pair x, y of its points, corresponds their *distance*, i.e., a non-negative real number $\rho(x, y)$ which satisfies the following conditions: a) $\rho(x, y) = 0$ if and only if $x = y$; b) $\rho(x, y) = \rho(y, x)$; c) $\rho(x, y) + \rho(y, z) \geqq \rho(x, z)$.

The operation of closure satisfying the conditions of Definition 11 can be introduced naturally into a metric space so that a metric space is transformed into a topological space. Let M be a subset and a a point of a metric space R. We shall call the *distance* from the point a to the set M the lower bound $\rho(a, M)$ of the numbers $\rho(a, x)$ for $x \varepsilon M$. The *closure* $\overline{M}$ of the set M is defined as the totality of all the points whose distance from M is equal to zero. A topological space in which the operation of closure can be defined in this way by means of a metric is called *metrizable.*

By the *sphere* of center a and radius $\epsilon > 0$ in a metric space R we understand the set of all points whose distance from a is less than ϵ. It follows that every sphere in R is an open set and that the aggregate of all spheres forms a basis of the topological space R.

Fundamental examples of metric spaces are the Euclidean spaces of finite dimension (see Example 13), and their generalization to infinitely many dimensions, known as Hilbert space H.

The elements of the space H are all the sequences $x = \{x_1, \cdots, x_n, \cdots\}$ of real numbers for which the series $x_1^2 + \cdots + x_n^2 + \cdots$ is convergent. Distance in H is defined by the relation

$$\rho(x, y) = \sqrt{[(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2 + \cdots]}.$$

9. Homeomorphism. Continuous Mapping

From the point of view of abstract topology two topological spaces having the same operation of closure are identical, or making use of the adopted terminology, homeomorphic. This is expressed more precisely in the following definition.

Definition 14. A mapping f of a topological space R on a topological space R' is called *homeomorphic* or *topological* if it is

1) one-to-one, and

2) preserves the operation of closure, i.e., for every $M \subset R$, we have $f(\overline{M}) = \overline{f(M)}$.

Obviously, if the mapping f is homeomorphic, then the inverse mapping f^{-1} is also homeomorphic.

Two topological spaces R and R' are called *homeomorphic* if one of them can be homeomorphically mapped on the other.

The concept of homeomorphism for topological spaces is an analogue of the concept of isomorphism for groups. As topological properties of topological

spaces we count only those which remain invariant under a homeomorphic mapping. It follows from Definition 14 that topological properties are those and only those which can be expressed in terms of closure. In this way the property of sets of being open or closed is topological, while the property of being a neighborhood is not topological, since an open set may enter into one basis of a space but not into another. In view of non-invariance of the concept of neighborhoods, we shall have to verify the topological invariance of all definitions formulated in terms of neighborhoods, i.e., if we replace a system of neighborhoods by an equivalent system the definition will have to remain unaltered (see §8, F)).

A weaker connection between two spaces than homeomorphic mapping is given by a continuous mapping. If homeomorphic mapping is an analogue of isomorphism, then continuous mapping is an analogue of homomorphism.

Definition 15. A mapping g of a topological space R into a topological space R' is called *continuous*, if for every $M \subset R$ we have

$$g(\overline{M}) \subset \overline{g(M)}.$$

A) We shall prove that if the mapping g is one-to-one and *bicontinuous*, i.e., if both g and g^{-1} are continuous, then g is homeomorphic.

Since the mapping g is continuous, $g(\overline{M}) \subset \overline{g(M)}$. We denote the set $g(M)$ by M', and applying to it the mapping g^{-1} we obtain $\overline{g^{-1}(M')} \subset g^{-1}(\overline{M}')$. But since the mapping g^{-1} is continuous, $g^{-1}(\overline{M}') \subset \overline{g^{-1}(M')}$. The last two relations taken together give $g^{-1}(\overline{M}') = \overline{g^{-1}(M')}$, i.e., the mapping g^{-1} is homeomorphic, since the set M, and hence also the set M', is arbitrary. Since g^{-1} is a homeomorphic mapping, g is also homeomorphic.

We now formulate the condition for continuous mapping in terms of neighborhoods. As a matter of fact this condition is rather important since it is used in practise to determine a continuous mapping.

Theorem 4. *In order that a mapping g of a space R into a space R' be continuous it is necessary and sufficient that the following condition be fulfilled: For every point $a \varepsilon R$ and every neighborhood U' of the point $a' = g(a) \varepsilon R'$ there exists a neighborhood U of the point a such that $g(U) \subset U'$.*

Proof. Suppose that the mapping g is continuous, and let U' be an arbitrary neighborhood of the point $a' = g(a)$. Put $F' = R' - U'$ and denote by F the complete inverse image of the set F' under the mapping g, $F = g^{-1}(F')$. Then F does not contain the point a.

Furthermore, because g is a continuous mapping we have $g(\overline{F}) \subset \overline{g(F)} \subset \overline{F}' = F'$, since F' is closed. Hence $\overline{F} \subset F$, i.e., F is also closed, and there exists a neighborhood U of the point a which does not intersect F, and this means that $g(U) \subset U'$. And so the necessity of the condition formulated above is established. We now prove its sufficiency. Suppose that this condition is fulfilled, and let $M \subset R$. We shall show that if $a \varepsilon \overline{M}$, then $a' = g(a) \varepsilon \overline{g(M)}$. Let U' be an arbitrary neighborhood of the point a'. Then by the condition above

there exists a neighborhood U of the point a such that $g(U) \subset U'$. Since $a \in \overline{M}$, U intersects M, but then U' intersects $g(M)$, i.e. $a' \in \overline{g(M)}$. Hence $g(\overline{M}) \subset \overline{g(M)}$.

We give two other necessary and sufficient conditions for a continuous mapping, which are also rather important.

Theorem 5. *In order that a mapping g of a space R in a space R' be continuous it is necessary and sufficient that one of the two following conditions be fulfilled:*

1) *If F' is a closed set of R', then the complete inverse image F of the set F' under the mapping g is a closed set in R.*

2) *If G' is an open set of R', then the complete inverse image G of the set G' under the mapping g is an open set in R.*

Proof. We shall show first of all that the conditions 1) and 2) are equivalent. Let F' and G' be two non-intersecting sets of R', whose sum is equal to R'. Let us denote by F and G the complete inverse images of the sets F' and G' under the mapping g. It is obvious that F and G do not intersect, and that their sum is equal to R. Suppose now that condition 1) is fulfilled and that G' is an arbitrary open set of R'. Then F' is a closed set (see Definition 12), and from condition 1) it follows that F is also closed, so that G is an open set. In this way 2) follows from 1). The fact that 1) follows from 2) can be proved in a similar way.

We shall now prove the necessity of condition 2). Let G' be an arbitrary open set of R' and G be the complete inverse image of G'. Let a be an arbitrary point of G and let $a' = g(a)$. Since G', is an open set, there exists a neighborhood U' of the point a' which is entirely contained in G' (see §8, G)). By Theorem 4 there exists a neighborhood U of the point a such that $g(U) \subset U'$, but since $U' \subset G'$ and G is the complete inverse image of G' we have $U \subset G$. Hence G is an open set (see §8 G)).

We finally prove the sufficiency of condition 2). Let a be an arbitrary point of R, $a' = g(a)$ and U' an arbitrary neighborhood of the point a'. Since U' is an open set in R', it follows from condition 2) that the complete inverse image G of the set U' under the mapping g is an open set in R, and hence there exists a neighborhood U of the point a which is entirely contained in G (see §8, G)). Hence $g(U) \subset U'$, and the mapping g is by reason of Theorem 4 continuous.

B) It is easy to see that if g is a continuous mapping of the space R in the space R', and g' is a continuous mapping of the space R' in the space R'', then the mapping $h(x) = g'(g(x))$ is also a continuous mapping of the space R in the space R''.

10. Subspace

If we want to carry out an analogy between the second and first chapters, then homeomorphic and continuous mappings become analogues of isomorphic and homomorphic mappings. We shall now proceed to construct an analogue of a subgroup.

Definition 16. Let R be a topological space, and R^* a subset of the set R. We can introduce a topology into R^* in a natural way by deducing it from the topology of the space R, so that the set R^* itself will become a topological space, a subspace of the space R. The concepts of closure, closed sets, and open sets, and other concepts which arise in this way in R^* are called *relative.* The relative operation of closure $\overline{M}^*$ of the set M in the space R^* is defined as follows: $\overline{M}^* = \overline{M} \cap R^*$.

Hence condition 1) of Definition 11 is fulfilled in R^*. We shall prove that conditions 2), 3), and 4) of this definition are also fulfilled.

If M contains only one element a, then $\overline{M}^* = \overline{M} \cap R^* = M \cap R^* = M$. Hence condition 2) holds.

Let M and N be two sets of R^*. Then

$$\overline{(M \cup N)}^* = \overline{(M \cup N)} \cap R^* = (\overline{M} \cup \overline{N}) \cap R^* = (\overline{M} \cap R^*) \cup (\overline{N} \cap R^*) = \overline{M}^* \cup \overline{N}^*,$$

i.e., condition 3) holds.

In proceeding to establish condition 4) we remark that it follows from the construction of the operation of closure in R^* that $N \subset \overline{N}^*$, since $\overline{N}^* = \overline{N} \cap R^* \supset N \cap R^* = N$. Furthermore, we have $\overline{M} \cap R^* \subset \overline{M}$, so that $\overline{\overline{M} \cap R^*} \subset \overline{M}$, and hence

$$\overline{\overline{M}^*}^* = \overline{\overline{M}^*} \cap R^* = \overline{(\overline{M} \cap R^*)} \cap R^* \subset \overline{M} \cap R^* = \overline{M}^*.$$

But we have just shown that $\overline{M}^* \subset \overline{\overline{M}^*}^*$, hence $\overline{\overline{M}^*}^* = \overline{M}^*$ and condition 4) holds.

We give now some elementary properties of subspaces.

A) Let R^* be a subspace of the space R (see Definition 16). If F is a closed set in R, then $E = F \cap R^*$ is a relative closed set in R^*, and conversely, every relative closed set E of R^* can be obtained as the intersection with R^* of some closed set F of R.

In fact, let F be a closed set of R and let $E = F \cap R^*$. Then $E \subset F$ and $\overline{E} \subset \overline{F} = F$. Taking intersections with R^* on both sides of the last relation we get $\overline{E} \cap R^* \subset F \cap R^*$, i.e., $\overline{E}^* \subset E$, but since $E \subset \overline{E}^*$, it follows that $\overline{E}^* = E$, and hence E is a relative closed set of R^*.

Conversely let E be a relative closed set of R^*. This implies that $E = \overline{E}^* = \overline{E} \cap R^*$, i.e., E is the intersection of a closed set $\overline{E}$ and R^*.

B) Let R^* be a subspace of the space R. If G is an open set of R, then $H = G \cap R^*$ is a relative open set of R^*. Conversely, every relative open set H of R^* can be obtained as the intersection with R^* of some open set G of R.

Let G be an arbitrary open set of R. Then $F = R - G$ is a closed set. Suppose that $H = G \cap R^*$ and $E = F \cap R^*$. It follows readily that $H = R^* - E$, but from what we have just shown (see A)), E is a relative closed set and hence H is a relative open set.

If conversely, H is a relative open set, then $E = R^* - H$ is a relative closed set and hence $E = F \cap R^*$, where F is closed in R (see A)). Then $G = R - F$ is an open set and $H = G \cap R^*$.

C) Let R be a topological space, R^* a subspace of R and Σ a basis of R. If we denote by Σ^* the totality of all sets of the form $G' \cap R^*$, where $G' \in \Sigma$, then Σ^* forms a basis of R^*. An analogous proposition holds for a basis about a point.

In fact since all the elements of Σ are open sets, it follows from what we have already shown (see B)) that Σ^* is composed of relative open sets. We shall prove that every relative open set H of R^* can be obtained as the sum of relative open sets belonging to the system Σ^*. We have shown (see B)) that $H = G \cap R^*$, where G is an open set. Since Σ is a basis of R, it follows that G can be written as the sum of some system Δ of open sets of Σ. We denote by Δ^* the totality of all sets of the form $G' \cap R^*$ with $G' \in \Delta$. Then $\Delta^* \subset \Sigma^*$ and H is the sum of all the sets contained in Δ^*.

D) Let R^* be a subspace of the space R. We shall associate with each point $x \in R^*$ the point $f(x) = x \in R$. Then the mapping f is a continuous mapping of the space R^* in the space R.

In order to prove this, we make use of condition 1) of Theorem 5 and remark A). If F is a subset of the space R, then the complete inverse image of the set F under the mapping f is $F \cap R^*$. If F is closed, then the set $F \cap R^*$ is closed in R^*, and hence the mapping f is continuous.

E) Let g be a continuous mapping of the space R in the space R'. Suppose that $g(R) \subset R^* \subset R'$. Since R^* is a subset of the space R', it is also a topological space. It follows that g is a continuous mapping of the space R in the space R^*.

To prove this it is sufficient to remark that if $F \subset R'$ then the complete inverse image of the set F under the mapping g coincides with the complete inverse image of $F \cap R^*$, and then to apply this remark to the case when F is closed.

Propositions D) and E) show that Definition 16 was given, so to speak, correctly. For if we were faced with the problem of assigning the topology of a subspace, we would aim to do so in such a way that propositions D) and E) would hold. It is interesting to notice that from this point of view the topology of a subspace is determined uniquely, that is, if we insist that propositions D) and E) be fulfilled, we will arrive at Definition 16.

Example 15. Let R be the totality of all real numbers. R can be treated as the set of all points on a line. We define in R the operation of closure as in Example 13 (for the case $n = 1$). Let R^* be the subspace of the space R which is composed of all numbers y such that $-1 < y < +1$. We shall show that R and R^* are homeomorphic. Let $y = (e^x - e^{-x})/(e^x + e^{-x})$. This relation associates every point x of the line R with some point of the interval R^*. This correspondence is one-to-one and bicontinuous.

Example 16. Let R be a plane with its usual topology (see Example 13). We denote by R^* the subspace of the space R which is composed of all points on the unit circle, i.e., of all points (x, y), which satisfy the equation $x^2 + y^2 = 1$. By R^{**} we denote the set of all points on the axis of abscissas whose abscissas φ satisfy $0 \leqq \varphi < 2\pi$. We obtain a one-to-one continuous mapping of the space

R^{**} on the space R^* by means of the relations $x = \cos \varphi$, $y = \sin \varphi$. It is not difficult to verify that this mapping is continuous and one-to-one. What is interesting is the fact that this mapping is not bicontinuous, i.e., the inverse mapping of the space R^* on the space R^{**} is not continuous. In fact the mapping has a discontinuity at the point whose coordinates are $(1, 0)$.

11. Connectedness

In this and the two following sections some additional restrictions will be pointed out which we shall impose at times on a general topological space. Connectedness is one of these restrictions which, however, does not play a very important rôle.

A) A topological space R is called *connected* if it cannot be decomposed into the sum of two non-null and non-intersecting closed sets A and B. Obviously the same definition can be given in still another form: a topological space R is *connected* if it cannot be decomposed into the sum of two non-null and non-intersecting open sets A and B.

Applying this definition to a subspace we obtain the concept of a connected set; namely, a set M of points of the space R is called *connected* when it can be thought of as a connected subspace (see Definition 16).

A more useful definition of a connected set can, however, be given directly as follows:

B) A subset M of a space R is called *connected* if it cannot be decomposed into the sum of two non-null and non-intersecting sets A and B which are such that $(\overline{A} \cap \overline{B}) \cap M$ is a null set. If $M = R$, then obviously this definition coincides with definition A).

C) Let Δ be the totality of connected subsets of the space R (see B)) which have a point a in common. Then the sum M of all the sets contained in Δ is connected.

Suppose that M is not connected. Then M can be decomposed into the sum of two non-null and non-interesting sets A and B which are such that $(\overline{A} \cap \overline{B}) \cap M$ is a null set. Let $a \varepsilon A$, $b \varepsilon B$, and P be an element of the system Δ which contains the point b. Let $A' = A \cap P$, and $B' = B \cap P$. Then A' and B' are two non-null and non-intersecting sets whose sum is P. Moreover, $\overline{A}' \subset \overline{A}$, $\overline{B}' \subset \overline{B}$ (see §7, B)), and $P \subset M$. We have therefore $(\overline{A}' \cap \overline{B}') \cap P \subset (\overline{A} \cap \overline{B}) \cap M$, but since the right side of this relation is zero by assumption, the left side is also zero. In this way P appears not to be connected, which contradicts the hypothesis.

D) Let a be a point of a topological space R. Then there exists in R a maximal connected subset K which contains the point a. The set K is a maximal set in the sense that every connected subset of the space R which contains a is in K. The set K is always closed and is called the *component* of the point a in the space R.

In fact let Δ be the totality of connected subsets of the space R which contain the point a. The sum K of all the sets contained in Δ is connected by

virtue of remark C)), and is by construction the maximal connected set which contains a. We shall show that the set K is closed. To do this, it is sufficient to show that $\overline{K}$ is connected, since in that case, K being a maximal set, we shall have $\overline{K} \subset K$, and hence $\overline{K} = K$ (see §7, A)). Suppose $\overline{K}$ were not connected. Then $\overline{K}$ is decomposable into the sum of two non-null and non-intersecting sets A and B such that $\overline{A} \cap \overline{B} \cap \overline{K}$ is null. Suppose that $A' = A \cap K$, $B' = B \cap K$, and that $a \varepsilon A'$. We shall then show that B' is empty. In fact, if B' is not empty, then K could be decomposed into the sum of two non-null and non-intersecting sets A' and B' such that $\overline{A}' \cap \overline{B}' \cap K$ is empty, since the last intersection is contained in $\overline{A} \cap \overline{B} \cap \overline{K}$, which is empty by hypothesis. Hence we have arrived at a contradiction and B' is empty. But this means that $K \subset A$ and hence the intersection $\overline{A} \cap \overline{B} \cap \overline{K} \supset \overline{K} \cap \overline{B} \cap \overline{K} = \overline{K} \cap \overline{B} \supset \overline{K} \cap B$ is not empty, since the set B is not empty and is contained in $\overline{K}$.

E) If there exists a continuous mapping g of a connected topological space R on some space R', then the space R' is connected.

Suppose the contrary were true. Then the space R' can be decomposed into two non-intersecting closed non-null subsets E' and F'. The inverse images E and F of these subsets in R are also closed (see Theorem 5) and add up to R. Hence the space R is decomposed into the sum of two non-intersecting non-null closed sets, which contradicts the assumption that R is connected.

12. Regularity. The Second Axiom of Countability

In this section we shall consider rather important further restrictions, namely regularity and the second axiom of countability, which we shall impose at times upon the topological spaces to be considered. Although we shall not make use of the first axiom of countability, in the future, we give it here for the sake of completeness.

We say that a topological space satisfies the *first axiom of countability* if each of its points admits a countable basis.

DEFINITION 17. A topological space R is called *regular* if for every neighborhood U of an arbitrary point a there exists a neighborhood V of the same point such that $\overline{V} \subset U$.

The invariance of this definition follows readily (see §8, F)). Let Σ and Σ' be two complete systems of neighborhoods of the space R (see Definition 13). Supposing that the system Σ is regular, we prove the regularity of the system Σ'. Let $U' \varepsilon \Sigma'$ be a neighborhood of the point a. Since Σ and Σ' are equivalent (see §8, F)), there exists a neighborhood $U \varepsilon \Sigma$ of the point a such that $U \subset U'$. Since Σ is regular, there exists a neighborhood $V \varepsilon \Sigma$ of the point a such that $\overline{V} \subset U$. Furthermore, because of the equivalence of Σ and Σ', we can find a neighborhood $V' \varepsilon \Sigma'$ of the point a such that $V' \subset V$, so that we have $\overline{V}' \subset \overline{V} \subset U \subset U'$, i.e., Σ' is regular.

In the future proofs of this type will be omitted because of their triviality.

A) In a regular space R each pair of distinct points a and a' have neighborhoods V and V' whose closures do not intersect.

Let U be a neighborhood of the point a which does not contain a' (see §8, D)). Since R is regular, there exists a neighborhood V of the point a such that $\overline{V} \subset U$. The open set $R - \overline{V}$ contains a', and therefore there exists a neighborhood U' of the point a' which is contained in $R - \overline{V}$. Because of regularity there also exists a neighborhood V' of the point a' such that $\overline{V}' \subset U'$. Obviously $\overline{V}$ and $\overline{V}'$ do not intersect.

DEFINITION 18. We say that the topological space R satisfies the *second axiom of countability* if it contains a basis having not more than a countable number of open sets (see Definition 13).

B) If a topological space R is regular then each of its subspaces R^* is regular, and if R satisfies the second axiom of countability then each of its subspaces satisfies the second axiom of countability (see Definition 16).

Suppose that R satisfies the second axiom of countability. Let Σ be a countable basis of the space R. The basis Σ^* of the subspace R^* which corresponds to the basis Σ (see §10, C)), is also countable, and hence R^* satisfies the second axiom of countability. Suppose that R is regular, and let $U^* = U \cap R^*$ be a neighborhood of the point a in the space R^*, while U is a neighborhood of this point in R. Since R is regular, there exists a neighborhood V of the point a in R such that $\overline{V} \subset U$. Suppose that $V^* = V \cap R^*$. Then $\overline{V}^* = \overline{(V \cap R^*)} \cap R^* \subset \overline{V} \subset U$, and $\overline{V}^* \subset R^*$, hence $\overline{V}^* \subset U^*$, i.e., the space R^* is regular.

In what follows in this section we shall consider only regular topological spaces which satisfy the second axiom of countability, although some of the propositions which we shall prove hold in a more general case. For brevity we introduce the following notation:

C) A regular topological space which satisfies the second axiom of countability will be called an *S-space.*

D) In an S-space R there exists for every point a a basis composed of open sets

$$W_1, \cdots, W_n, \cdots \tag{1}$$

which are such that

$$\overline{W}_{n+1} \subset W_n, \qquad n = 1, 2, \cdots. \tag{2}$$

Let Σ be a countable basis of the space R. We denote by $U_1, \cdots, U_n, \cdots$ the open sets of Σ which contain the point a, and by V_n the intersection of all the open sets $U_1, \cdots, U_n$. It is easy to see that the open sets

$$V_1, \cdots, V_n, \cdots \tag{3}$$

form a basis about the point a, with $V_{n+1} \subset V_n$, $n = 1, 2, \cdots$. In fact, if G is any open set containing the point a, there exists a number p such that $U_p \subset G$, but then also $V_p \subset G$. We now select from the sequence 3) the sequence 1), i.e., $W_i = V_{n_i}$, $i = 1, 2, \cdots$, which satisfies condition 2). To do this suppose that $W_1 = V_1$, and that the open set W_i is already chosen. Because of regular-

ity, there exists a number $n_i + k$ for which $\overline{V}_{n_i+k} \subset V_{n_i}$. Letting $W_{i+1} = V_{n_i+k}$, the sequence 1) is determined by induction.

We shall now introduce the concept of a convergent sequence of points. This concept could be introduced into an arbitrary topological space, but in all its generality it does not prove valuable. We shall use it only in connection with S-spaces.

E) We say that a sequence of points

$$4) \qquad a_1, \cdots, a_n, \cdots$$

of an S-space R *converges to the point* a of this space if for every neighborhood U of the point a there exists an integer k such that U contains all the points a_n of the sequence 4), with $n > k$. In particular, all the points of sequence 4) may coincide with the point b, in which case $a = b$.

F) If in an S-space R the sequence 4) converges to a, then the set N of points of this sequence cannot have a limit point $a' \neq a$. Furthermore, the sequence (4) cannot converge to a point $a'' \neq a$.

In fact, let V and V' be two non-intersecting neighborhoods of the points a and a' (see A)). Since the sequence (4) converges to a, it follows that all of its points, except a finite number, belong to V, and hence a' cannot be a limit point of N. In the same way we can prove that the sequence (4) cannot converge to a''.

G) Let R be an S-space and let $M \subset R$. The point $a \varepsilon R$ belongs to $\overline{M}$ if and only if M contains a sequence of points which converges to a.

For if M contains a sequence which converges to a, then every neighborhood of the point a intersects M, and hence $a \varepsilon \overline{M}$ (see §8, C)). If conversely $a \varepsilon \overline{M}$, we construct for a the basis (1) which satisfies condition (2). Since every neighborhood W_n of the point a intersects M (see §8, C)), there exists a point $a_n \varepsilon W_n$ which belongs to M. It is easy to see that the sequence $a_1, \cdots, a_n, \cdots$ thus obtained converges to a.

H) Let R be a topological space which satisfies the second axiom of countability, let M be one of its subsets, and let Ω be a set of open sets whose sum contains M. Then we can select from the system Ω, a countable system Ω' of open sets whose sum also contains M.

In short, from an arbitrary covering we can always select a countable covering.

Let Σ be a countable basis of the space R. Denote by $\Sigma' = \{U_1, U_2, \cdots, U_n, \cdots\}$ the totality of all open sets of Σ which are such that each of them is contained in at least one open set of the system Ω. Every open set G of the system Ω can be represented as the sum of some system Σ_G of open sets of Σ. But since each open set of the system Σ_G is contained in G, $\Sigma_G \subset \Sigma'$. Hence every open set of Ω can be represented as a sum of open sets of Σ'. Because the system Ω covers M, the system Σ' possesses the same property. Denote by G_n an open set of the system Ω which contains the open set U_n. The sys-

tem $\Omega' = \{G_1, \cdots, G_n, \cdots\}$ covers the set M. Hence from an arbitrary covering Ω we have selected a countable covering Ω'.

EXAMPLE 17. Let R be the topological space defined in Example 12. Since a complete system of neighborhoods Σ of R can be assigned in such a way that every open set of Σ contains only one point, the regularity is obvious. On the other hand, if R contains a non-countable number of points, the second axiom of countability is not satisfied, since every basis of the space R must contain all the open sets having one point each.

EXAMPLE 18. Let R be the topological space defined in Example 11. Every non-null open set G of R can be obtained by removing from R a finite set N, $G = R - N$. It follows from this directly that R satisfies the second axiom of countability if and only if the number of points in R does not exceed a countable number, and that R is regular only if it has a finite number of points. In fact, let a be a point and U a neighborhood of a. Let V be another neighborhood of a. If R contains an infinite number of points, then $\overline{V} = R$, and hence $\overline{V} \subset U$ only when $U = R$, but, of course, every point a has a neighborhood U distinct from R.

13. Compactness

We shall consider here the rather important restricting condition of compactness, which we shall impose at times on the topological spaces under consideration. It is worth noting that the condition of compactness alone is not a sufficient restriction, and, therefore we shall discuss primarily compact S-spaces (see §12, C)). Together with compactness an important part is played by local compactness.

DEFINITION 19. A subset M of a topological space R is called *compact* if every infinite subset $N \subset M$ has at least one limit point in M. A topological space R is called *compact*, if the set R is itself compact. A topological space R is called *locally compact* if each of its points has a neighborhood whose closure is compact.

A) A closed subset M of a compact topological space R is compact. In particular it follows that every compact space is at the same time locally compact.

For, every infinite subset $N \subset M$ has a limit point in R since R is compact; but since M is closed, this limit point belongs to M.

B) Every compact subset M of an S-space is closed.

Suppose the contrary to be true. Then there exists a point a contained in $\overline{M}$ but not belonging to M. By §12, G), M contains a sequence

$$a_1, \cdots, a_n, \cdots, \tag{1}$$

which converges to a. But (1) has to contain an infinite number of distinct points, for in the contrary case all the points of the sequence 1), with only a finite number of exceptions, will have to concide with a. But a does not belong to M. Hence (1) is an infinite set, and as such must have a limit point in M,

but its only limit point is the point a (see §12, F)). Hence $a \varepsilon M$, which contradicts the assumption.

THEOREM 6. *Let*

2) $$F_1, \cdots, F_n, \cdots$$

be a sequence of compact non-null subsets of an S-space such that $F_{n+1} \subset F_n$, $n = 1, 2, \cdots$. *Then the intersection* F *of all sets of the sequence* 2) *is non-empty and compact.*

PROOF. If the sequence 2) is stationary beginning with a certain subscript i, i.e., if $F_n = F_{n+1}$ for every $n \geqq i$, then $F = F_i$, and F_i is by assumption not empty. If this does not happen, then we can choose from the sequence 2) a subsequence

3) $$E_1, \cdots, E_n, \cdots$$

such that $E_{n+1} \neq E_n$, with $E_{n+1} \subset E_n$, $n = 1, 2, \cdots$. Let $a_n \varepsilon E_n - E_{n+1}$. All the points a_n, $n = 1, 2, \cdots$, are distinct and therefore the set $M_n = \{a_n, a_{n+1}, \cdots\}$ is infinite. We remark that the limit points of the sets M_i and M_j coincide because these sets differ by only a finite number of points. We shall therefore designate the totality of limit points, of M_i by N. The set N is not empty, since E_i is compact. Furthermore $N \subset E_i$, since $M_i \subset E_i$, and E_i, being compact, is closed (see B)). Hence $N \subset F$ and F is non-empty. Being the intersection of closed sets of the sequence (2), F is closed, and being a subset of a compact set F_1, the set F is also compact (see A)).

As a consequence of Theorem 6, we prove the following proposition.

C) If G is an open set containing the intersection F of the sets of sequence 2) (see Theorem 6), then there exists a number k such that for every $n \geqq k$, we have $F_n \subset G$.

We shall suppose that $E_n = F_n - G$, and show that E_n is compact. For the sets $R - G$ and F_n are closed (see B)), and hence their intersection E_n is closed. But, being a closed subset of a compact space F_n, the set E_n must be compact (see A)). We have $E_{n+1} \subset E_n$, $n = 1, 2, \cdots$. If all sets E_i of the sequence

4) $$E_1, \cdots, E_n, \cdots,$$

with i exceeding some integer n, are zero, then the assertion C) is proved; if all the sets of the sequence 4) are non-empty, then the intersection E is also non-empty (see Theorem 6). It is easy to see that $E = F - G$, but since we have supposed that $F \subset G$, it follows that E is empty, i.e., we have arrived at a contradiction.

THEOREM 7. *Let* R *be an S-space,* M *a compact subset of* R *and* Ω *a system of open sets whose sum contains* M. *We can then select from the system* Ω *a finite system of open sets whose sum contains* M. *In short, we can select from an arbitrary covering* Ω *a finite covering.*

Proof. From the covering Ω we select a countable covering

$$\Omega' = \{G_1, \cdots, G_n, \cdots\}$$

(see §12, H)). Suppose that $H_n = G_1 \cup G_2 \cup \cdots \cup G_n$, and $F_n = M - H_n$. Then $F_{n+1} \subset F_n$ and F_n is compact, $n = 1, 2, \cdots$ (see B), A)). If beginning with a certain number k, all sets of the sequence

5) $$F_1, \cdots, F_n, \cdots$$

are empty, then $H_k \supset M$, and hence a finite system $G_1, \cdots, G_k$ of open sets of Ω covers M, i.e., the theorem is already proved. If all the sets of the sequence 5) are non-empty, then their intersection is also non-empty by Theorem 6. This means that there exists a point in M which does not belong to any open set of the system Ω', which contradicts the condition that Ω' covers the set M.

Theorem 8. *Let f be a continuous mapping of a compact space R on R'. Then R' is also compact. If, moreover, the mapping f is one-to-one, and if R' is an S-space, then f is a topological mapping.*

Proof. If R' is non-compact, then there exists in R' an infinite subset N' having no limiting point in R'. We shall show that this is impossible. We select for every point x' of the set N', a point x of R such that $f(x) = x'$. The totality of all points x thus obtained we denote by N. Then N is an infinite set and has a limit point a in R, since R is compact. We shall show that $a' = f(a)$ is a limit point of the set N'. Let U' be an arbitrary neighborhood of the point a', and let U be a neighborhood of a for which $f(U) \subset U'$. Such a neighborhood exists, since $f(x)$ is continuous (see Theorem 4). Since a is a limit point of the set N, there exist in U two distinct points p and q of N. The points $f(p)$ and $f(q)$ are distinct and both belong to U'. Hence at least one of these points is distinct from a and belongs to both U' and N', so that a' is a limit point of N', and we have arrived at a contradiction.

Suppose now that the mapping $f(x)$ is one-to-one, and that R' is an S-space. We shall show that in this case the inverse mapping $f^{-1}(x')$ is also continuous. To do this, it is sufficient to show that if F is an arbitrary closed subset of R, then its complete inverse image F' is closed under the mapping $f^{-1}(x')$ (see Theorem 5). Since $f(x)$ is one-to-one, it follows that $F' = f(F)$. But F, being a closed subset of a compact space, is compact. We have in this way a continuous mapping of a compact space F on the space F', and hence, by what we have just shown, F' is compact. But as such, it is closed in R' (see B)).

D) If

6) $$a_1, \cdots, a_n, \cdots$$

is a sequence of points of a compact S-space R, then we can select from it a convergent sequence.

Let N be the set of all points of the sequence 6). If the set N is finite, then the sequence 6) has an infinite number of points which coincide with some

point a. The points of the sequence 6), which coincide with a form a subsequence which converges to a. Suppose now that N is infinite. Then N has a limit point a, and it follows from remark G) of §12 that three exists a sequence of points of N which converges to a. This gives us the desired subsequence.

For many constructions of converging sequences in mathematics the so-called *diagonal process* is often used. We shall formulate it here by means of the following theorem.

THEOREM 9. *Let $R^1, \cdots, R^i, \cdots$ be a sequence of compact S-spaces, and let a_n^i, $n = 1, 2, \cdots, i = 1, 2, \cdots$, be a system of points such that $a_n^i \varepsilon R^i$. Then it is possible to select an increasing sequence $n(1), n(2), \cdots, n(k), \cdots$ of natural numbers such that for a fixed i, every sequence $a_{n(1)}^i, a_{n(2)}^i, \cdots, a_{n(k)}^i, \cdots$ converges in the space R^i.*

PROOF. Since the space R^1 is compact, it follows from D) that there exists an increasing sequence

$$n(1, 1), n(1, 2), \cdots, n(1, k), \cdots \tag{7}$$

of natural numbers such that the sequence $a_{n(1,k)}^1$, $k = 1, 2, \cdots$, converges in R^1. Since the space R^2 is compact, we can select from the sequence 7), a subsequence $n(2, 1), n(2, 2), \cdots, n(2, k), \cdots$ of natural numbers such that the sequence of points $a_{n(2,k)}^2$, $k = 1, 2, \cdots$, converges in R^2. Continuing this process of selection we construct increasing sequences $\Delta^i = \{n(i, 1), n(i, 2), \cdots, n(i, k), \cdots\}$ of natural numbers, which are such that the sequence of points

$$a_{n(i,k)}^i, \qquad k = 1, 2, \cdots, \tag{8}$$

converges in R^i, for $i = 1, 2, \cdots$, and the sequence Δ^{i+1} is a subsequence of the sequence Δ^i. We now write $n(k) = n(k, k)$, and let $\Delta = \{n(1), n(2), \cdots, n(k)\}$. If we strike out the first $i - 1$ terms from the sequence Δ, we obtain a sequence which is a subsequence of the sequence Δ^i, and since the sequence of points 8) converges, it follows that the sequence $a_{n(k)}^i$, $k = 1, 2, \cdots$, also converges. Hence we have constructed the desired increasing sequence of natural numbers.

EXAMPLE 19. Let R be a Euclidean space with its usual topology (see Example 13). It is easy to see that R is regular, and that it satisfies the second axiom of countability. But R is not compact, since there exists in it an infinite sequence of points having no limit point. However, every closed bounded subset of the space R is compact. And conversely, every compact subset of R is a closed bounded set.

14. Continuous Functions

In what follows an important rôle will be played by continuous functions defined on a topological space. It is easy to prove for these functions the usual propositions of analysis concerning continuous functions (see below, A) and B)). The main purpose of this section is to give a proof of a rather important and non-trivial lemma of Urysohn.

DEFINITION 20. We say that a real-valued *function* $f(x)$ is defined on a topological space R if to every element $x \varepsilon R$ corresponds a real number $f(x)$. The function $f(x)$ is called *continuous at the point* a, if for every positive number ϵ there exists a neighborhood U of the point a such that for every $x \varepsilon U$ we have $|f(x) - f(a)| < \epsilon$. The function $f(x)$ is called *continuous* if it is continuous at every point x of the space R.

This definition expresses with precision the fact that the function $f(x)$ gives a continuous mapping of a topological space R in the space of real numbers (see Definition 15)

A) Let $f(x)$ be a continuous real-valued function defined on a connected topological space (see §11, A)). If the function $f(x)$ assumes the values a and b, then it assumes every intermediary value c, $a < c < b$.

For if we assume the contrary to be true, it will follow that a continuous function $f(x)$ gives a mapping of a connected topological space R on a non-connected set of real numbers, which is impossible (see §11, E)).

B) A real-valued function $f(x)$ given on a compact topological space R (see Definition 19) is bounded and achieves its maximum and minimum.

We denote by R' the set of all values assumed by the function $f(x)$, $R' = f(R)$. The set R', being an aggregate of real numbers, is a topological space. Since R is compact, it follows from Theorem 8 that R' is also compact. As a compact set of real numbers R' must be closed and bounded, and hence the function $f(x)$ is bounded. We now denote by s and t the greatest lower and least upper bounds of the set R'. Since R' is bounded and closed, s and t belong to R', and hence the function $f(x)$ achieves its maximum and minimum.

Propositions A) and B) make it clear what type of lemmas we shall use to prove some of the well known theorems of analysis concerning continuous functions.

URYSOHN'S LEMMA. *Let R be a compact regular topological space satisfying the second axiom of countability* (see Definitions 17, 18, 19) *and let E and F be two of its non-intersecting closed subsets. Then there exists a continuous function $f(x)$ defined on G such that $0 \leqq f(x) \leqq 1$ for every $x \varepsilon R$, $f(x) = 0$ for every $x \varepsilon E$, and $f(x) = 1$ for every $x \varepsilon F$.*

The idea of the proof of this lemma depends on the following construction. Every binary fraction r, $0 < r < 1$ is put into correspondence with an open set G_r of the space R such that $E \subset G_r$ and $\overline{G}_r$ does not intersect F. Moreover, $\overline{G}_{r'} \subset G_{r''}$ if $r' < r''$. After such a system of open sets has been constructed, the construction of the function can be accomplished without difficulty.

PROOF. We show first of all that if A and B are two non-intersecting closed subsets of R, then there exists an open set G such that $A \subset G$, and $\overline{G}$ does not intersect B.

Let x be an arbitrary point of A, and $R - B$ an open set containing x. Since R is regular there exists a neighborhood U_x of the point x such that $\overline{U}_x \subset R - B$, i.e., $\overline{U}_x$ does not intersect B. When x assumes all the values of the set A, the

system of open sets U_x covers A. Being a closed subset of a compact space, A is compact (see §13, A)). By Theorem 7 we can select from the covering of the set A by open sets U_x a finite covering $U_1, U_2, \cdots, U_k$. The sum $G = U_1 \cup U_2 \cup \cdots \cup U_k$ contains A, and $\overline{G}$ does not intersect B since $\overline{G} = \overline{U}_1 \cup \overline{U}_2 \cup \cdots \cup \overline{U}_k$, and $\overline{U}_i$ does not intersect B for any i.

We now construct in R a finite system Σ_n of open sets G_r, where r is a rational number, written in the form $q/2^n$, $q = 1, 2, \cdots, 2^n - 1$, and possessing the following properties: a) $E \subset G_r$, $\overline{G}_r$ does not intersect F, b) for $r' < r''$, $\overline{G}_{r'} \subset G_{r''}$.

We shall carry out the construction by induction on n, and Σ_{n+1} will be obtained by enlarging Σ_n.

Σ_1 contains only one open set $G_{\frac{1}{2}}$. To construct $G_{\frac{1}{2}}$ we let $A = E$ and $B = F$. Then by what we have just proved, there exists an open set G such that $A \subset G$, and $\overline{G}$ does not intersect with B. Let $G_{\frac{1}{2}} = G$, then condition a) for Σ is satisfied, while condition b) has as yet no meaning.

Suppose that Σ_n is already constructed, we then proceed to construct Σ_{n+1}. Let $r = q/2^{n+1}$. If q is even, let $q = 2p$; then $r = p/2^n$ and we have in this case $G_r \varepsilon \Sigma_n$, so that G_r has already been constructed. Now let $q = 2p + 1$, and let $s = p/2^n$ and $t = (p + 1)/2^n$. We have to distinguish three cases: 1) $s > 0$, $t < 1$; in this case G_s and G_t have already been constructed, and we can let $A = \overline{G}_s$, $B = R - G_t$, then A and B are closed non-intersecting sets, since $\overline{G}_s \subset G_t$. 2) $s = 0$; in this case G_t exists and we let $A = E$, $B = R - G_t$, and A and B are closed non-intersecting sets since $E \subset G_t$. 3) $t = 1$; then G_s exists and we let $A = \overline{G}_s$, $B = F$, and A and B are again two closed non-intersecting sets since $\overline{G}_s$ and F do not intersect. It follows that in all three cases there exists an open set G such that $A \subset G$, and $\overline{G}$ does not intersect B. Let $G_r = G$; in this way the system of open sets Σ_{n+1} is constructed.

We now show that in the system Σ_{n+1} thus constructed condition a) is satisfied. In case 1) we have $E \subset G_s \subset G_r$, $\overline{G}_r \subset G_t \subset R - F$, and hence $E \subset G_r$ and $\overline{G}_r$ does not intersect F. In case 2) $E \subset G_r$ and $\overline{G}_r \subset G_t \subset R - F$, and hence $E \subset G_r$ and $\overline{G}_r$ does not intersect F. Finally in case 3) $E \subset G_s \subset G_r$, while $\overline{G}_r \subset R - F$, and hence $E \subset G_r$ and $\overline{G}_r$ does not intersect F. Hence condition a) is satisfied.

We now pass to condition b). Let $r' < r''$, where $r' = q'/2^{n+1}$ and $r'' = q''/2^{n+1}$. If q' and q'' are both even, then $G_{r'}$ and $G_{r''}$ belong to Σ_n, and hence by the hypothesis of the induction $\overline{G}_{r'} \subset G_{r''}$. Let $q' = 2p'$, $q'' = 2p'' + 1$, and let $s = p''/2^n$. Then $r' \leqq s$ and we have $\overline{G}_{r'} \subset \overline{G}_s \subset G_{r''}$, i.e., $\overline{G}_{r'} \subset G_{r''}$. If $q' = 2p' + 1$, and $q'' = 2p''$, we let $t = (p' + 1)/2^n$. Then $t \leqq r''$ and we have $\overline{G}_{r'} \subset \overline{G}_t \subset G_{r''}$, i.e., $\overline{G}_{r'} \subset G_{r''}$. If $q' = 2p' + 1$, $q'' = 2p'' + 1$, we let $s = p''/2^n$. Then $r' < s$ and we have $\overline{G}_{r'} \subset G_s \subset G_{r''}$, i.e., $\overline{G}_{r'} \subset G_{r''}$. Hence condition b) is also fulfilled.

Let now Σ' be the totality of all open sets which belong to all the systems Σ_n, $n = 1, 2, \cdots$. We enlarge Σ' by the open set $G_1 = R$, and denote this enlarged system by Σ''. Then Σ'' contains all the open sets G_r where r is an arbitrary binary fraction not exceeding unity. Also $E \subset G_r$ and $\overline{G}_r$ does not intersect F, with the single exception when $r = 1$; moreover $\overline{G}_{r'} \subset G_{r''}$ for $r' < r''$.

Let x be an arbitrary point of R. We denote by $f(x)$ the lower bound of all values of r for which $x \varepsilon G_r$. The function $f(x)$ thus obtained satisfies the conditions of the lemma. In fact, if $x \varepsilon E$, then $x \varepsilon G_r$ for every r, and since the lower bound of all possible values of r is zero, $f(x) = 0$. If $x \varepsilon F$, then $x \varepsilon G_r$ only when $r = 1$, and hence $f(x) = 1$. Moreover, since r takes on only positive values not exceeding unity, it is true for all values of x that $0 \leqq f(x) \leqq 1$. We shall now prove the continuity of $f(x)$ for an arbitrary point $x = a$ in R. Let ϵ be an arbitrary positive number. Let us first suppose that $f(a) = 0$. Let r be a positive binary fraction less than ϵ. Then $a \varepsilon G_r$. We denote by U a neighborhood of a such that $U \subset G_r$. Then for any $x \varepsilon U$ we have $f(x) \leqq r \leqq \epsilon$ since $x \varepsilon G_r$, but since $f(x) \geqq 0$, $|f(x) - f(a)| < \epsilon$. Let $f(a) > 0$ and let r, s, and t be three positive binary fractions not exceeding unity, and such that $f(a) - \epsilon < r < s < f(a) \leqq t < f(a) + \epsilon$. Obviously a does not belong to G_s, and since $r < s$, a does not belong to $\overline{G}_r$, but $a \varepsilon G_t$. Hence a belongs to the open set $G_t - \overline{G}_r$. We denote by U a neighborhood of the point a such that $U \subset G_t - \overline{G}_r$. For every $x \varepsilon U$ we have $r \leqq f(x) \leqq t$ and hence $|f(x) - f(a)| < \epsilon$. It follows that the function $f(x)$ is continuous.

We remark that in the construction of $f(x)$ the compactness of R was used only in the first point of the proof.

EXAMPLE 20. We give here by way of an example a brief exposition of a theorem of Urysohn having to do with metrizability.

In connection with Example 14, the question naturally arises under what conditions a space R is metrizable. It turns out that a compact topological space R is metrizable if and only if it is regular and satisfies the second axiom of countability. We shall sketch here the proof of only the following proposition:

A compact regular topological space R satisfying the second axiom of countability is metrizable.

Let Σ be a countable basis of the space R. We denote by (U_n, V_n), $n = 1, 2, \cdots$, the totality of all pairs of open sets of the system Σ such that $\overline{U}_n$ and $\overline{V}_n$ do not intersect. Let $E = \overline{U}_n$ and $F = \overline{V}_n$ and denote by $f_n(x)$ the continuous function constructed in Urysohn's lemma for the sets E and F. We associate with every point $x \varepsilon R$ the sequence of numbers $x_n = (1/n)f_n(x)$, $n = 1, 2, \cdots$. We also associate with every point $x \varepsilon R$ the point $g(x) = \{x_1, \cdots, x_n, \cdots\}$ of Hilbert space (see Example 14). The mapping g of the space R on Hilbert space turns out to be continuous and one-to-one. Hence by Theorem 8 the space R is homeomorphically mapped on a subspace R' of the Hilbert space, and hence R is homeomorphic with a metric space R'.

15. Topological Products

Some analogies between the theory of topological spaces and the theory of groups have been pointed out before. This analogy is most pronounced in the concept of topological product, which appears to be an exact repetition of the concept of direct product.

DEFINITION 21. Let R and S be two topological spaces. From them we construct a new topological space T called the *topological product* of the spaces R and S, $T = R \cdot S$. By a point of the space T we understand any pair of points (x, y) where $x \varepsilon R$ and $y \varepsilon S$. The topology of T can be given by means of the definition of a topological space based on neighborhoods. Let $M \subset R$ and $N \subset S$. We define as the *product* of the sets M and N the set $P = M \cdot N$ composed of all pairs (x, y) where $x \varepsilon M$ and $y \varepsilon N$; then $M \cdot N \subset R \cdot S$. If now Σ is a basis of R and Σ' a basis of S, we define the basis Σ'' of the space T as the totality of all sets of the form $W = U \cdot V$, where $U \varepsilon \Sigma$, and $V \varepsilon \Sigma'$.

The topological space T is given by means of the defining system of neighborhoods Σ'' (see §8, E)). We now have to show that the conditions of Theorem 3 hold for the system Σ''.

Let (x, y) and (x', y') be two distinct points of T. Then either $x \neq x'$ or $y \neq y'$. Suppose that $x \neq x'$, and let U be a neighborhood of the point x not containing x', and V be an arbitrary neighborhood of y. The product $U \cdot V$ gives a neighborhood of the point (x, y) not containing (x', y'). Hence condition a) of Theorem 3 is satisfied.

Let $U \cdot V$ and $U' \cdot V'$ be two neighborhoods of the point (x, y) in the space T. We denote by U'' a neighborhood of the point x such that $U'' \subset U \cap U'$, and by V'' a neighborhood of y such that $V'' \subset V \cap V'$. Then the neighborhood $U''\ V''$ of the point (x, y) satisfies the relation $U''\ V'' \subset U \cdot V \cap U' \cdot V'$ and hence condition b) of Theorem 3 is also satisfied.

It is not hard to see that the definition of topological product given here is a topological invariant, i.e., if we replace the systems Σ and Σ' by equivalent systems, Σ'' will also be replaced by an equivalent system (see §8, F)).

A) If G is an open set of the space R and H an open set of the space S, then the product $G \cdot H$ is an open set of the space T.

For, let (x, y) be a point of $G \cdot H$, so that $x \varepsilon G$, $y \varepsilon H$, and there exist neighborhoods U and V of the points x and y such that $U \subset G$, and $V \subset H$. But then $U \cdot V$ is a neighborhood of the point (x, y) belonging to $G \cdot H$ and hence $G \cdot H$ is an open set (see §8, G)).

B) If E and F are two closed sets of the spaces R and S, then the product $E \cdot F$ is a closed set in T.

Let $G = R - E$ and $H = S - F$. It can readily be seen that $E \cdot F = R \cdot S - (G \cdot S \cup R \cdot H)$. But $G \cdot S$ and $R \cdot H$, being products of open sets, are themselves open sets and hence $E \cdot F$ is closed in $R \cdot S$.

C) If the second axiom of countability holds in R and S it also holds in T. This follows directly from the construction of a basis for T.

D) If R and S are regular, then their product T is also regular.

Let (x, y) be a point in T and let $U \cdot V$ be one of its neighborhoods in the system Σ''. Since R and S are regular, there exist neighborhoods U' and V' of the points x and y such that $\overline{U}' \subset U$, $\overline{V}' \subset V$. Then $U' \cdot V' \subset \overline{U}' \cdot \overline{V}' \subset U \cdot V$. Since $\overline{U}' \cdot \overline{V}'$ is the product of two closed sets, it is also closed and hence $\overline{U'V'} \subset \overline{U}' \cdot \overline{V}'$, and $\overline{U'V'} \subset U \cdot V$.

E) If R and S are compact regular topological spaces satisfying the second axiom of countability then their product T is compact.

Let M be an infinite set of T. We shall prove that M has a limit point in T. Without loss of generality we may suppose that M is countable, for if M were non-countable, we could prove the existence of a limit point for some countable subset of M. Let us number all the points of M, $M = \{c_1, c_2, \cdots, c_n, \cdots\}$ and let us suppose that $c_n = (a_n, b_n)$. Since R is compact, regular, and satisfies the second axiom of countability, we can select from the sequence $a_1, \cdots, a_n, \cdots$ a convergent subsequence $a_{n_1}, \cdots, a_{n_i}, \cdots$ (see §13, D)), converging to the point a. Since S is compact, regular, and satisfies the second axiom of countability, we can select from the sequence $b_{n_1}, \cdots, b_{n_i}, \cdots$ a convergent subsequence. Let this subsequence converge to the point b. Then it follows readily that the point $c = (a, b)$ is a limit point for the set M.

F) If R and S are locally compact, regular, and satisfy the second axiom of countability, then their product T is also locally compact.

Let $c = (a, b)$ be a point of T. Since R and S are locally compact, there exist neighborhoods U and V of the points a and b such that $\overline{U}$ and $\overline{V}$ are compact. It follows from what we have already proved that $\overline{U} \cdot \overline{V}$ is compact and closed, hence $\overline{UV} \subset \overline{U} \cdot \overline{V}$, and therefore $\overline{UV}$, being a closed subset of a compact space $\overline{U} \cdot \overline{V}$, must be compact. Hence the product $U \cdot V$ is a neighborhood of the point c whose closure is compact, and therefore T is locally compact.

We note that we can determine without difficulty the product of an arbitrary finite number of topological spaces.

The concept of a topological product is useful for the discussion of functions of many variables.

G) Let R and S be two topological spaces. We say that $f(x, y)$ is a *real-valued function of two variables* $x \varepsilon R$ and $y \varepsilon S$, if to every pair $x \varepsilon R$ and $y \varepsilon S$ corresponds a real number $f(x, y)$. The function $f(x, y)$ is called *continuous* for $x = a$ and $y = b$ if for every positive ϵ there exist neighborhoods U and V of the points a and b such that for $x \varepsilon U$ and $y \varepsilon V$ we have $|f(x, y) - f(a, b)| < \epsilon$. The function $f(x, y)$ is called *continuous* if it is countinuous for every pair of values $x = a \varepsilon R$, $y = b \varepsilon S$.

We now denote by T the topological product of R and S. The function $f(x, y)$ of two variables $x \varepsilon R$ and $y \varepsilon S$ can be treated as a function $f(z)$ of a single variable $z = (x, y) \varepsilon T$, $f(z) = f(x, y)$. Conversely the function $f(z)$ of a single variable $z = (x, y) \varepsilon T$ can be treated as a function $f(x, y)$ of two variables $x \varepsilon R$ and $y \varepsilon S$, $f(x, y) = f(z)$. Thus a continuous function $f(x, y)$ corresponds to a continuous function $f(z)$ and conversely a continuous function $f(z)$ corresponds to a continuous function $f(x, y)$.

If the spaces R and S coincide, we arrive at the concept of a function of two variables belonging to the same space.

In this way, making use of the topological product, we reduce the concept of continuity for a function of many variables to the concept of continuity of a function of one variable.

EXAMPLE 21. We shall discuss here the concept of a topological product of a system of compact, regular, topological spaces, satisfying the second axiom of countability.

Let $R_1, \cdots, R_n, \cdots$, be a countable sequence of compact regular topological spaces satisfying the second axiom of countability. Let us define their topological product. We take for a point x of the product T any countable sequence $x = \{x_1, \cdots, x_n, \cdots\}$, where $x_n \varepsilon R_n$, $n = 1, 2, \cdots$. We define an arbitrary neighborhood U in T from a finite system of neighborhoods $U_1, \cdots, U_k$, where $U_i \subset R_i$, $i = 1, \cdots, k$, by saying that $x \varepsilon U$ if $x_i \varepsilon U_i$, $i = 1, \cdots, k$.

It is not hard to show that the conditions of Theorem 3 are satisfied for the system of neighborhoods of the space T which we have defined here.

We can also show easily that the product T thus defined is regular and satisfies the second axiom of countability. The proof of compactness of the space T can be carried out by means of the diagonal process (see Theorem 9).

EXAMPLE 22. The topological product of two Euclidean spaces R^m and R^n of dimensions m and n is homeomorphic with the Euclidean space of dimensionality $m + n$.

The coordinate method itself is a concrete application of the concept of a topological product. A plane can be regarded as the product of two straight lines, a three-space as the product of three straight lines, and so on.

CHAPTER III

TOPOLOGICAL GROUPS

From the point of view of logic, the concept of topological group is a simple combination of the concepts of abstract group and topological space. The operations of group multiplication and of topological closure can be assigned simultaneously in the same set G. These operations are, however, not independent, but are connected by the condition of continuity: the group operations operating in G must be continuous in the topological space G. Because of such a definition the concept of a topological group is not at all specific in the first stages of its development. The fundamental relations holding for abstract groups and topological spaces are more or less bodily carried over into topological groups. In this way we have here the subgroup, the normal subgroup, the factor group, etc. A few particular situations arise, but they are comparatively superficial. This chapter is devoted to the exposition of these rather general, and non-specific properties of topological groups. A deeper study of topological groups will be made later.

Historically, the concept of a topological group arose in connection with the consideration of groups of continuous transformations. If some continuous manifold, such as a Euclidean space, for instance, is subjected to a group of continuous transformations, then some limiting relations arise naturally in the group itself, and it is transformed into a topological group. In this way, originally, a topological group was treated as a group of continuous transformations. Further developments in this field have shown, however, that the most interesting of the properties studied are not connected with the fact that the group under consideration is a group of continuous transformations, but depend only on the limiting relations taking place in the group itself. This is why it is useful to give first the theory of topological groups without treating them as groups of transformations, and only later to point out, by way of application, the connection with continuous transformations.

16. The Concept of a Topological Group

We shall give here the definition of a topological group and indicate its simplest properties.

DEFINITION 22. A set G of elements is called a *topological group* if

1) G is an abstract group (see Definition 1),

2) G is a topological space (see Definition 11),

3) the group operations in G are continuous in the topological space G. In greater detail this condition can be formulated as follows (see Definition 13, and §2, A)):

a) If a and b are two elements of the set G, then for every neighborhood W

of the element ab there exist neighborhoods U and V of the elements a and b such that $UV \subset W$.

b) If a is an element of the set G, then for every neighborhood V of the element a^{-1} there exists a neighborhood U of the element a such that $U^{-1} \subset V$.

It is not hard to show that conditions a) and b) can be replaced by the single condition:

c) If a and b are two elements of the set G, then for every neighborhood W of the element ab^{-1} there exist neighborhoods U and V of the elements a and b such that $UV^{-1} \subset W$.

The topological invariance of this definition, i.e., the independence of condition 3) of the choice of the defining system of neighborhoods can readily be shown (see §8, F)).

We shall now determine some rather elementary properties of topological groups.

A) Let $a_1, \cdots, a_n$ be a finite system of elements of a topological group G, let $a_1^{r_1} \cdots a_n^{r_n} = c$ be a product of powers of the a's, where the powers may be positive or negative, and let W be an arbitrary neighborhood of the element c. Then there exist neighborhoods $U_1, \cdots, U_n$ of the elements $a_1, \cdots, a_n$ such that $U_1^{r_1} \cdots U_n^{r_n} \subset W$, where U_i is taken equal to U_j if $a_i = a_j$, the same being true for a greater number of equal elements.

This assertion can be proved by a successive application of condition 3) of Definition 22 together with condition b) of remark D) of §8.

B) Suppose that $f(x) = xa$, $f'(x) = ax$, $\varphi(x) = x^{-1}$, where a is a fixed element of the group G, and x a variable element of this group. Then each of the functions $f(x)$, $f'(x)$ and $\varphi(x)$ is a topological mapping of the space G into itself (see Definition 14).

We shall prove this only for $f(x)$. First, $f(x)$ is one-to-one. In fact for every element y' there exists one and only one element x' such that $y' = x'a$. Furthermore, the mapping $f(x)$ is continuous. For if $y' = x'a$ and W is some neighborhood of y', then by condition 3) of Definition 22 there exist neighborhoods U and V of the elements x' and a such that $UV \subset W$; but $a \varepsilon V$, so that $Ua \subset W$, i.e., $f(U) \subset W$, which proves the continuity of the mapping $f(x)$ (see Theorem 4). The continuity of the inverse mapping $f^{-1}(y) = ya^{-1}$ can be proved in the same way.

C) Let F be a closed set, U an open set, P an arbitrary set, and a some element of the group G. Then Fa, aF, F^{-1} are all closed sets, while UP, PU, U^{-1} are open sets (see §2, A)).

This assertion follows from B). For the mapping $f(x) = xa$ is a topological mapping and therefore a closed set F goes into a closed set $f(F) = Fa$. In the same way it can be shown that the set Ua is an open set, but then UP is a sum of open sets and, therefore, also an open set.

D) A topological group G is *homogeneous*. This means that for any two elements p and q of the group G there exists a topological transformation $f(x)$ of the space G into itself which transforms p into q.

To prove this it is sufficient to let $a = p^{-1}q$, for then the topological transformation $f(x)$ defined in B) satisfies the condition $f(p) = q$.

E) From the homogeneity of a topological group G it follows that it is sufficient to state and verify its local properties for a single element only. For instance, in order to make sure that the space G is locally compact it is sufficient to show that its identity e admits a neighborhood U whose closure is compact. Regularity may be verified in the same way. Moreover, if the identity e admits a neighborhood containing e alone, then every element of G has a neighborhood consisting of a single element.

F) The topological space G of a topological group G is regular (see Definition 17).

By remark E) the regularity of the space G can be established by considering the neighborhoods of the identity e. Let U be a neighborhood of e. Since $ee^{-1} = e$, it follows from A) that there exists a neighborhood V of the identity such that $VV^{-1} \subset U$. We shall show that $\bar{V} \subset U$. Let ρ be a point of $\bar{V}$. Then every neighborhood of the point ρ intersects V (see §8, C)). It follows from C) that ρV is a neighborhood of ρ and hence there exists in V a point b such that $\rho b = a \varepsilon V$, but then $\rho = ab^{-1} \varepsilon VV^{-1} \subset U$, and this means that $\bar{V} \subset U$.

G) Let G be a topological group satisfying the second axiom of countability, and let P and Q be two of its compact subsets; then the product PQ is compact (see Definitions 18 and 19, and also §2, A)).

Let $c_1, \cdots, c_n, \cdots$ be an infinite sequence of elements of the set PQ. Every element c_n can be written in the form $c_n = a_nb_n$, $a_n \varepsilon P$, $b_n \varepsilon Q$. Since G satisfies the second axiom of countability and is regular by F), it follows that from the sequence $a_1, \cdots, a_n, \cdots$ a subsequence $a_{n_1}, \cdots, a_{n_i}, \cdots$ can be selected which converges to some element $a \varepsilon P$ (see §13, D)). The sequence $b_{n_1}, \cdots, b_{n_i}, \cdots$ has a limit point b in Q. It follows readily that the sequence $c_{n_1}, \cdots, c_{n_i}, \cdots$ has the limit point ab. This can be proved using condition 3) of Definition 22.

17. Systems of Neighborhoods of the Identity

It follows from the considerations of the previous section that condition 3) of Definition 22 establishes a very close connection between algebraic and topological operations in a topological group G. Because of this it follows, in particular, that if the algebra of G is given then in order to define the topology of G it is not necessary to give a basis of the whole space G (see Definition 13), but it is sufficient to assign a complete system of neighborhoods of the identity (see §8, B′)). The simplest illustration of this fact is afforded by the so-called discrete groups.

A) A topological group G is called *discrete* if it contains no limit elements, i.e., if each of its elements has a neighborhood containing only a single point. It follows from remark E) of §16 that a topological group G is discrete if and only if its identity is an isolated element of the group.

It is easy to see that a topology can be introduced into any abstract group G whatsoever in such a way that G becomes a discrete group. It follows therefore that the theory of discrete groups coincides with the theory of abstract groups.

The question of how the topology of a group G may be determined by a complete system of neighborhoods of the identity, and how, in general, a topology may be introduced into an abstract group is answered by remark C) and Theorem 10. Before taking up these propositions, however, we introduce an important topological notion.

B) A subset M of a topological space R is called *everywhere dense* in R if the closure $\overline{M}$ of the set M coincides with R, $\overline{M} = R$. It is clear that M is everywhere dense in R if and only if every open set of R intersects M.

C) Let G be a topological group, Σ^* a complete system of neighborhoods of its identity e, and M a set everywhere dense in G. Then the totality Σ of all sets of the form Ux where $U \varepsilon \Sigma^*$, $x \varepsilon M$, forms a complete system of neighborhoods of the space G, while the system Σ^* satisfies the following conditions:

a) The only element common to all the sets of the system Σ^* is e.

b) The intersection of any two sets of the system Σ^* contains a third set of the system Σ^*.

c) For every set U of the system Σ^* there exists a set V of the same system such that $VV^{-1} \subset U$.

d) For every set U of the system Σ^* and element $a \varepsilon U$ there exists a set V of the system Σ^* such that $Va \subset U$.

e) If U is a set of the system Σ^* and a an arbitrary element of the group G, then there exists a set V of the system Σ^* such that $a^{-1}Va \subset U$.

We shall first prove proposition C). It follows from remark C) of §16 that the sets of the system Σ are open sets of the space G. We shall show that the system Σ forms a basis of the space G. Let W be an arbitrary open set of the space G and let $a \varepsilon W$. Then Wa^{-1} is an open set containing the identity, and hence by §16, A), there exists a neighborhood U of the identity e ($U \varepsilon \Sigma^*$) such that $UU^{-1} \subset Wa^{-1}$. Since the set M is everywhere dense in G, it follows that aM^{-1} is also everywhere dense in G, and hence there exists an element d which belongs to both U and aM^{-1}. We note that then $d^{-1}a \varepsilon M$. But then $Ud^{-1}a \varepsilon \Sigma$. On the other hand, since $UU^{-1} \subset Wa^{-1}$, and since $d \varepsilon U$, we have $Ud^{-1} \subset Wa^{-1}$, and this means that $Ud^{-1}a \subset W$. Furthermore, since $d \varepsilon U$, it follows that $e \varepsilon Ud^{-1}$, and hence $a \varepsilon Ud^{-1}a$. In this way the completeness of the system Σ is established (see §8, B)).

As to the five conditions a), $\cdots$, e), conditions a) and b) are fulfilled in any topological space (see §8, D)), while conditions c), d), and e) follow from remark A) of §16.

THEOREM 10. *Let G be an abstract group, and Σ^* a system of subsets of G which satisfies the five conditions of remark C). Then a topology can be introduced into the group G uniquely in such a way that the group operations in G are continuous*

in this topology, and the system Σ^* may be taken as a complete system of neighborhoods of the identity. In other words, the abstract group G admits one and only one topologization under which the system Σ^* is a complete system of neighborhoods of the identity.

PROOF. If the group G can be topologized in such a way that Σ^* is a complete system of neighborhoods of the identity, then by remark C) a complete system of neighborhoods of a topological space G can be composed of all sets of the form Ux, where $U \varepsilon \Sigma^*$ and $x \varepsilon G$. We denote by Σ the totality of all sets of this form, and show first that Σ satisfies the conditions of Theorem 3, and second that the group operations in G are continuous in the topology thus obtained.

Let a and b be two distinct elements of the group G. Since the intersection of all sets of the system Σ^* contains only e, there exists a $U \varepsilon \Sigma^*$ such that ba^{-1} does not belong to U; but then Ua does not contain b. Hence condition a) of Theorem 3 is satisfied.

To prove that condition b) is satisfied we note first of all that if $b \varepsilon Ua$, where $U \varepsilon \Sigma^*$, then there exists a $V \varepsilon \Sigma^*$ such that $Vb \subset Ua$. In fact $ba^{-1} \varepsilon U$, and by condition d) there exists a $V \varepsilon \Sigma^*$ such that $Vba^{-1} \subset U$, but then $Vb \subset Ua$.

Let now Ua and Vb be two neighborhoods of the point c, i.e., $c \varepsilon Ua$, and $c \varepsilon Vb$, $U \varepsilon \Sigma^*$, and $V \varepsilon \Sigma^*$. From what we have just remarked there exist $U' \varepsilon \Sigma^*$ and $V' \varepsilon \Sigma^*$ such that $U'c \subset Ua$ and $V'c \subset Vb$. Since by condition b) there exists a $W \varepsilon \Sigma^*$ which is contained in the intersection of U' and V', it follows that $Wc \subset Ua$, and $Wc \subset Vb$. But Wc is a neighborhood of c and hence the condition b) of theorem 3 is also fulfilled.

We shall show now that the operations of the group G are continuous in the topology thus obtained.

Let $c = ab^{-1}$ and $W'c'$ be a neighborhood of the point c. By what has already been shown there exists a $W \varepsilon \Sigma^*$ such that $Wc \subset W'c'$. By condition c) there exists a $U \varepsilon \Sigma^*$ such that $UU^{-1} \subset W$. Furthermore, by condition e) there exists a $V \varepsilon \Sigma^*$ such that $ab^{-1}Vba^{-1} \subset U$. But then $ab^{-1}V^{-1} \subset U^{-1}ab^{-1}$ and hence

$$Ua(Vb)^{-1} = Uab^{-1}V^{-1} \subset UU^{-1}ab^{-1} \subset Wab^{-1} = Wc \subset W'c'.$$

Hence condition 3) of Definition 22 is fulfilled.

Therefore, the abstract group G with the topology introduced by the system of neighborhoods Σ is a topological group.

We shall now show that Σ^* is a basis about the point e (see §8, B)). Let W be an arbitrary open set of the space G containing e. Since Σ is a basis of the space G, there exists a neighborhood $Ua \varepsilon \Sigma$ of the point e such that $Ua \subset W$ (see §8, B)). From $e \varepsilon Ua$ it follows that $a^{-1} \varepsilon U$, and hence by condition d) there exists a $V \varepsilon \Sigma^*$ such that $Va^{-1} \subset U$, i.e., $V \subset Ua \subset W$, and since $e \varepsilon V$, this implies that Σ^* is a basis about the point e.

We now show that if a topology T is given in a group G under which the

system Σ^* can be taken as a complete system of neighborhoods of the identity, then this topology T coincides with the topology constructed by means of the system Σ. To prove this, it is sufficient to show that the system Σ can be taken as a complete system of neighborhoods in the topology T.

By assumption Σ^* is a complete system of neighborhoods in the topology T, and hence all the sets of the system Σ^* are open sets in the topology T. Then all the sets of the system Σ are also open sets (see §16, C)) .Let now W be an open set in the topology T which contains a. Then Wa^{-1} contains e and is (by §16, remark C)) also an open set. Since Σ^* is a complete system of neighborhoods of the identity, there exists in Σ^* an open set U such that $U \subset Wa^{-1}$, but then $Ua \subset W$. Hence the system Σ gives a complete system of neighborhoods in the topology T (see §8, B)).

Example 23. Let G be the additive group of whole numbers. We introduce into G a series of different topologies.

Let p be a prime number. We denote by U_k the set of all whole numbers which are divisible by p^k. We take for a complete system of neighborhoods of zero the totality Σ^* of all sets U_k, $k = 1, 2, \cdots$.

It can easily be verified that all the conditions imposed by Theorem 10 on the system Σ^* are satisfied. Let us verify only c). If $a \varepsilon U_k$ and $b \varepsilon U_k$, then $a - b \varepsilon U_k$. In this way condition c) holds here in a particularly simple manner.

It is clear that the topologies obtained by the above method for two distinct prime numbers p and p' are distinct. In fact the sequence $p, p^2, \cdots, p^k, \cdots$ converges to zero under the first topology, but does not converge to zero under the second.

Example 24. The set of vectors of the r-dimensional Euclidean space forms an additive group. In Example 13 we introduced a topology into the space of these vectors. It can easily be verified that the operation of addition of vectors is continuous in the topology thus defined. We therefore obtain the topological group of vectors of r-dimensional Euclidean space, or the r-dimensional vector group.

Example 25. Let G be the set of all square matrices of order n with determinants different from zero. In example 2 we define a multiplication in G. Let us now introduce a topology into G as follows: we denote by Φ_k the set of all matrices of G whose elements do not exceed $1/k$ in absolute value, and by U_k the set of all matrices of G of the form $a + e$, where e is the unit matrix, and $a \varepsilon \Phi_k$. By Σ^* we denote the totality of all sets U_k, $k = 1, 2, \cdots$. It is not hard to show that the system Σ^* satisfies all the conditions of Theorem 10, and therefore the set G is topologized.

18. Subgroup. Normal Subgroup. Factor Group

In this section we extend to topological groups the results obtained for abstract groups in section 2.

Definition 23. Let G be a topological group. A set H of elements of G

is called a *subgroup of the topological group* G if a) H is a *subgroup* of the *abstract* group G (see Definition 2), b) H is a *closed* subset of the *topological* space G (see Definition 12). A subgroup N of a topological group G is called a *normal subgroup* of G if N is a normal subgroup of the abstract group G (see Definition 3).

Thus, the fact that G is not merely an abstract group but is further a topological group imposes on H and N only the one additional condition of topological closure.

A) Let H be a subset, not necessarily closed, of a topological group G, and let H be a subgroup of the abstract group G. Then H is a topological group because of the topology which arises in H as a subspace of the space G (see Definition 16). In particular a subgroup H of a topological group G is itself a topological group.

To prove this it is sufficient to show that the group operations in H are continuous in the topological space H. Let a and b be two elements of the set H and let $ab^{-1} = c$. Every neighborhood W' of the element c in the space H can be obtained as the intersection with H of some neighborhood W of the element c in the space G, $W' = H \cap W$ (see §10, B)). Since G is a topological group, there exist neighborhoods U and V of the elements a and b such that $UV^{-1} \subset W$. Now $U' = H \cap U$ and $V' = H \cap V$ are relative neighborhoods of the elements a and b in the space H. We have $U'V'^{-1} \subset W$, and also $U'V'^{-1} \subset H$; hence $U'V'^{-1} \subset W'$, i.e., condition 3) of Definition 22 is satisfied for the group H.

B) Let G be a topological group and H one of its subgroups. If G is compact or locally compact, then H is respectively compact or locally compact (see Definition 19).

If G is compact, then H, as a closed subset of G, is also compact (see §13, A)). If G is locally compact and if $a \varepsilon H$, then there exists a neighborhood U of the element a in G such that its closure $\overline{U}$ is compact. The intersection $H \cap U = U'$ is a relative neighborhood of the element a in the space H. Since H is closed in G, it follows that $\overline{U}' \subset H$, and hence $\overline{U}'^* = \overline{U}' \cap H = \overline{U}'$. Furthermore, $\overline{U}' \subset \overline{U}$, and therefore $\overline{U}'$ is compact, as a closed subset of a compact set. Hence H is locally compact.

In §2 we established the concept of cosets of a general subgroup H in the group G. In the case of abstract groups the set of all cosets of a subgroup H presented nothing of interest from our point of view. If, on the other hand, we are concerned with a topological group, then the totality of cosets forms here in a natural way a topological space which plays an important role.

DEFINITION 24. Let G be a topological group and H one of its subgroups. We denote by G/H the totality of all right cosets of the subgroup H in the group G (see §2, D)). We introduce a topology into the set G/H as follows. Let Σ be a complete system of neighborhoods of the space G (see Definition 13) and let $U \varepsilon \Sigma$. Denote by U^* the set of all cosets of the form Hx, where $x \varepsilon U$. For the system Σ^* of neighborhoods of the space G/H we take the totality of all

sets of the form U^*, where U is an arbitrary element of Σ. The topological space G/H thus obtained we shall call the *space of right cosets* of the subgroup H in the group G. Analogously we define the space of left cosets and use the symbol G/H for it also. In the cases where there is no danger of ambiguity we shall make no distinction between the spaces of left and right cosets.

It is easy to show that the definition of topology in the space G/H given here is invariant, i.e., it does not depend on the choice of the system Σ (see §8, F)).

We shall now show that the system Σ^* satisfies the conditions of Theorem 3.

Let A and B be two distinct cosets and let $a \in A$. Since $B = Hb$ is a closed set (see §16, C)) and a does not belong to B, there exists a neighborhood U of the element a which does not intersect B. Then the set U^* of all the cosets of the form Hx, where $x \in U$, forms a neighborhood of the coset A which does not contain B. Hence condition a) of Theorem 3 is fulfilled.

Let now U^* and V^* be two neighborhoods of a coset A, and let $a \in A$. U^* is the set of all cosets of the form Hx, where $x \in U$, $U \subset \Sigma$, while V^* is composed of all cosets of the form Hy, where $y \in V$, $V \subset \Sigma$. HU and HV are open sets in G containing a (see §16, C)). Hence there exists a neighborhood W of the element a which is contained in both open sets HU and HV. We denote by W^* the set of all cosets of the form Hz, where $z \in W$. It follows readily that W^* is a neighborhood of the coset A which is contained in the intersection $U^* \cap V^*$. Hence condition b) of Theorem 3 is also satisfied.

C) The mapping f of a topological space R into a topological space R' will be called *open* if every open set U of the space R goes over into an open set under the mapping f, i.e., $f(U)$ is an open set. The mapping f is open if and only if for every point $a \in R$ and every neighborhood V of a there exists a neighborhood V' of the point $f(a) = a'$ such that $V' \subset f(V)$.

For, if the mapping f is open, then the existence of the desired neighborhood V' is obvious, since $f(V)$ is an open set containing the point a'. Suppose now that the assumption that V' exists is satisfied for every point a and every neighborhood V of a. Let U be an open set of the space R. We shall show that $f(U)$ is an open set. Let $a' \in f(U)$. Then $a' = f(a)$, where $a \in U$. Let us denote by V a neighborhood of the point a which is contained in U; such a neighborhood exists, since U is an open set. Then, by assumption, there exists a neighborhood V' of the point a' such that $V' \subset f(V)$. Since $V \subset U$, $f(V) \subset f(U)$ and hence $V' \subset f(U)$, and $f(U)$ is an open set (see §8, G)).

THEOREM 11. *Let G be a topological group, H one of its subgroups and G/H the space of cosets* (see Definition 24). *We associate with every element x of the space G the element $X = f(x)$ of the space G/H which is the coset containing the element x. The mapping f of the topological space G on the space G/H is a continuous open mapping.*

This mapping will be called the *natural* mapping of the space G on the space G/H.

PROOF. Let us suppose for the sake of definiteness that G/H is the space of right cosets. Let $a \varepsilon G$, and $A = Ha$, so that $f(a) = A$. Further let U^* be some neighborhood of the element A of the space G/H. U^* is composed of all cosets of the form Hx, where $x \varepsilon U$, and U is a neighborhood of a in the space G. HU is an open set in G containing the element a (see §16, C)). Hence there exists a neighborhood V of the element a which is contained in HU. It follows readily that $f(V) \subset U^*$. Hence the mapping f is continuous (see Theorem 4).

Let $a \varepsilon G$, and $A = Ha = f(a)$. Denote by U some neighborhood of the element a. The set of all cosets of the form Hx, where $x \varepsilon U$, forms a neighborhood U^* of the element A. We have $f(U) = U^*$, and hence $U^* \subset f(U)$. Hence the mapping f is open (see C)).

The most important case arises when H is a normal subgroup. In this case we have the following definition:

DEFINITION 25. Let G be a topological group and N a normal subgroup G. The set G/N of cosets is an abstract group by Definition 4, and at the same time the set G/N is a topological space by Definition 24. It will be shown that the group operations in G/N are continuous in the topological space G/N. Hence G/N is a topological group. It is called the *factor group* of the topological group G by the normal subgroup N.

We first prove the continuity of the group operations in G/N.

Let A and B be two elements of G/N, $C = AB^{-1}$, and W^* a neighborhood of the element C. W^* is composed of all the cosets of the form Nz, where $z \varepsilon W$, and W is a neighborhood in G. Since $C \varepsilon W^*$, there exists an element $c \varepsilon W$ such that $C = Nc$. Let b be an arbitrary element of B and $a = cb$; then $a \varepsilon A$. Since the group operations in G are continuous, there exist neighborhoods U and V of the elements a and b such that $UV^{-1} \subset W$. Let us denote by U^* the neighborhood of the element A which is composed of all cosets of the form Nx, where $x \varepsilon U$, and by V^* the neighborhood of the element B composed of all cosets of the form Ny, where $y \varepsilon V$. We have then

$$Nx(Ny)^{-1} = Nxy^{-1}N^{-1} = NN^{-1}xy^{-1} = Nxy^{-1} \varepsilon W.^*$$

Hence $U^*V^{*-1} \subset W^*$, i.e., condition 3) of Definition 22 is satisfied and the group operations are continuous in G/N.

D) Let G be a topological group and G/N one of its factor groups. If G satisfies the second axiom of countability, so does G/N (see Definition 18).

The proof of this proposition follows from Definitions 24 and 25.

E) If a topological group G is compact or locally compact, then each of its factor groups G/N is correspondingly compact or locally compact.

In case G is compact the statement follows from Theorems 8 and 11. Suppose now that G is locally compact. Then there exists a neighborhood U of the identity e such that its closure $\overline{U}$ is compact. Let f be the natural mapping of the space G on the space G/N (see Theorem 11). Since f is an open mapping (see C)), it follows that $f(U) = U^*$ is an open set in G/N. Since f is continuous $f(\overline{U})$ is compact (see Theorem 8). Furthermore $N \varepsilon U^*$, and because of the

regularity of G/N (see §16, F)) there exists a neighborhood V^* of the element N such that $\bar{V}^* \subset U^* \subset f(\bar{U})$. Since $\bar{V}^*$ is a closed subset of the compact set $f(\bar{U})$, it is also compact. Hence by remark E) of §16 the space G/N is locally compact.

F) Let G be a topological group satisfying the second axiom of countability. If a normal subgroup N and the corresponding factor group $G/N = G^*$ are both compact, then G itself is compact.

Let $a_1, \cdots, a_n, \cdots$ be a sequence of elements of the group G. We shall show that we can select from it a convergent subsequence. We denote by f the natural mapping of the group G on the group G^* (see Theorem 11), and let $a_n^* = f(a_n)$. Since the group G^* is compact, we can select from the sequence $a_1^*, \cdots, a_n^*, \cdots$ a subsequence which converges to some element a^*. In order not to change notation we shall suppose simply that the sequence $a_1^*, \cdots, a_n^*, \cdots$ itself converges to a^*.

We now denote by $U_1, \cdots, U_n, \cdots$ some decreasing sequence of neighborhoods of the identity e in G which forms a basis about e. Taking $U_n^* = f(U_n)$, it follows that the sequence $U_1^*, \cdots, U_n^*, \cdots$ is also decreasing, and forms a complete system of neighborhoods of the identity e^* in the group G^*. Replacing the sequence $a_1, \cdots, a_n, \cdots$ by one of its subsequences, we can arrive at the relation $a_n^* a^{*-1} \varepsilon U_n^*$, $n = 1, 2, \cdots$. We shall denote an inverse image of the point a^* in the group G by a', and an inverse image of the point $a_n^* a^{*-1}$ in the neighborhood U_n by b_n. We also set $a_n' = b_n a'$. Then the sequence $a_1', \cdots, a_n', \cdots$ converges to a', and $f(a_n') = f(a_n)$, $n = 1, 2, \cdots$.

Let us now suppose that $c_n = a_n a_n'^{-1}$. Then the sequence $c_1, \cdots, c_n, \cdots$ belongs to N, and therefore we can select from it a converging subsequence. In order not to change notation we shall again suppose that the sequence $a_1, \cdots, a_n, \cdots$ has been replaced by a subsequence for which $c_1, \cdots, c_n, \cdots$ converges. Since the sequences $a_1', \cdots, a_n', \cdots$ and $c_1, \cdots, c_n, \cdots$ converge, it follows that the sequence

$$a_1 = c_1 a_1', \cdots, a_n = c_n a_n', \cdots$$

also converges. Hence by replacing the sequence $a_1, \cdots, a_n, \cdots$ by its subsequences several times we finally arrive at a convergent sequence, and hence we have established the compactness of the group G.

G) Every topological group G has two trivial normal subgroups. These are the subgroup $\{e\}$ consisting only of the identity, and the whole group G. In contradistinction to the terminology established for the theory of abstract groups (see §2, G)), the topological group G is called *simple* only if each of its normal subgroups is either discrete or coincides with G (see §17, A)). In general, discrete normal subgroups play a special part in the theory of topological groups.

We conclude with one more remark.

H) Let G be a topological group, and H a subgroup or a normal subgroup of

the abstract group G. Then $\bar{H}$ is respectively a subgroup or a normal subgroup of the topological group G.

Suppose that $a \varepsilon \bar{H}$, and $b \varepsilon \bar{H}$. We then prove that $ab^{-1} \varepsilon \bar{H}$. Let W be a neighborhood of the element ab^{-1}. Then there exist neighborhoods U and V of the elements a and b such that $UV^{-1} \subset W$. Since $a \varepsilon \bar{H}$ and $b \varepsilon \bar{H}$ there exist elements x and y of H such that $x \varepsilon U$ and $y \varepsilon V$; but then $xy^{-1} \varepsilon H$, and at the same time $xy^{-1} \varepsilon W$. Hence an arbitrary neighborhood W of the element ab^{-1} intersects H, and $ab^{-1} \varepsilon \bar{H}$. Accordingly $\bar{H}$ is a subgroup of the abstract group G. But since $\bar{H}$ is closed in the space G, it follows that $\bar{H}$ is a subgroup of the topological group G.

Now let H be a normal subgroup of the abstract group G, and let $a \varepsilon \bar{H}$, and $c \varepsilon G$. Let V be an arbitrary neighborhood of the element $c^{-1}ac$. Then there exists a neighborhood U of the element a such that $c^{-1}Uc \subset V$. Since $a \varepsilon \bar{H}$, there exists an element x in H belonging to U. Furthermore $c^{-1}xc \varepsilon H$ and $c^{-1}xc \varepsilon V$, i.e., an arbitrary neighborhood V of the element $c^{-1}ac$ intersects H and therefore $c^{-1}ac \varepsilon \bar{H}$. Hence $\bar{H}$ is a normal subgroup of the topological group G.

Example 26. Let G be the additive group of all real numbers. This set G of all real numbers forms a topological space. It is not hard to verify that we have here a topological group.

Let us make clear what subgroups the group G admits. Let H be a subgroup of the group G. If H contains elements different from zero, then it contains a positive number d. If d can be chosen arbitrarily small then its multiples will fill out G arbitrarily densely, and since H is closed, we shall have $G = H$. Hence if $H \neq G$, then there exists in H a least positive number h. It is not hard to show that in this case H consists of all multiples of h, and hence H is a discrete subgroup of the group G. Therefore, G is a simple topological group (although it is not a simple abstract group).

A typical example of a discrete subgroup N of the group G is the set of all whole numbers. The factor group G/N is homeomorphic with the circle. It is easy to see that G/N is also a simple group.

Example 27. Let G be the r-dimensional vector group (see Example 24). We select in G a coordinate system and denote by N the set of all elements with integral coordinates. It can be seen readily that N is a discrete normal subgroup of the group G, and that the factor group G/N is compact.

19. Isomorphism. Automorphism. Homomorphism

In this section we generalize to topological groups the concepts and relations which have been established for abstract groups in section 3.

From the point of view of our theory two topological groups are the same if they possess the same topological and algebraic structures. In greater detail this thought is expressed in the following definition.

Definition 26. A mapping f of a topological group G on a topological group G' is called *isomorphic* if

1) f is an isomorphic mapping of the abstract group G on the abstract group G' (see Definition 5),

2) f is a homeomorphic mapping of the topological space G on the topological space G' (see Definition 14).

Two topological groups are called *isomorphic* if there exists an isomorphic mapping of one group on the other.

We shall show below by examples that two topological groups may be isomorphic as abstract groups, but not isomorphic as topological groups.

A) An isomorphic mapping of a topological group G into itself is called an *automorphism* of the group G. As in section 3, the set of all automorphisms of a topological group G forms an abstract group. We shall not discuss here the question of introducing a topology into the group of automorphisms of a topological group.

Definition 27. A mapping g of a topological group G into a topological group G^* is called *homomorphic* if

1) g is a homomorphic mapping of the abstract group G into the abstract group G^* (see Definition 6),

2) g is a continuous mapping of the topological space G into the topological space G^* (see Definition 15).

A homomorphic mapping g of a topological group G into a topological group G^* is called *open* if g is an open mapping of the topological space G into the topological space G^* (see §18, C)).

The distinction between open and non-open homomorphisms is quite essential in the theory of topological groups. It is the open homomorphism which gives a natural generalization of the concept of homomorphism in the theory of abstract groups.

B) Let G and G^* be two topological groups, and let g be a homomorphic mapping of the abstract group G into the abstract group G^*. In order that the mapping g should be continuous or open it is sufficient that it should be such at the identity e of the group G, i.e., it is sufficient in order that g be *continuous* that

a) for every neighborhood U^* of the identity e^* of the group G^* there exist a neighborhood U of the identity e such that $g(U) \subset U^*$;

and in order that g be *open* that

b) for every neighborhood V of the identity e there exist a neighborhood V^* of the identity e^* such that $g(V) \supset V^*$.

Suppose that condition a) is fulfilled. Let $a \in G$, $g(a) = a^*$ and let U^* be an arbitrary neighborhood of the element a^*. Then U^*a^{*-1} is a neighborhood of the unit e^*, and hence from condition a) there exists a neighborhood U' of the identity e such that $g(U') \subset U^*a^{*-1}$. Since $U = U'a$ is a neighborhood of the element a we have $g(U) = g(U')g(a) \subset U^*a^{*-1}a^* = U^*$. Hence the mapping g is continuous. Analogously, it follows from condition b) that the mapping g is open.

C) Let G be a topological group, N one of its normal subgroups and G/N

the corresponding factor group. Let us associate with every element $x \varepsilon G$ that coset X of the normal subgroup N which contains x, $x \varepsilon X$, $g(x) = X$. Then the mapping g of the topological group G on the topological group G/N is an open homomorphic mapping. We shall call this mapping the *natural homomorphic mapping* of the group G on the group G/N.

We have shown in §3 that g is a homomorphic mapping of the abstract group G on the abstract group G/N (see §3, C)). In §18 it was shown that g is an open continuous mapping of the topological space G on the topological space G/N (see Theorem 11). It follows, therefore, from Definition 27 that g is an open homomorphic mapping of the topological group G on the topological group G/N.

A proposition inverse to C) may be stated in the following theorem.

THEOREM 12. *Let G and G^* be two topological groups, let g be an open homomorphic mapping of the group G on the group G^* and let N be the kernel of the homomorphism g. Then N is a normal subgroup of the group G, and the topological group G^* is isomorphic with the group G/N. The isomorphism established here between the groups G^* and G/N coincides with the isomorphism of Theorem 1.*

We shall call it the *natural* isomorphism.

PROOF. By Theorem 1, N is a normal subgroup of the abstract group G. Furthermore, since N is a complete inverse image of the element e^* under the continuous mapping g, it follows from Theorem 5 that N is a closed subset of the topological space G. Hence N is a normal subgroup of the topological group G.

Let x^* be an element of the group G^*, and X the totality of all the elements of G which go into x^* under the mapping g. It was shown in Theorem 1 that X is a coset of N in the group G. Let us suppose that $f(x^*) = X$. As was shown in Theorem 1, f is an isomorphic mapping of the abstract group G^* on the abstract group G/N. We shall show that f is a homeomorphic mapping of the space G^* on the space G/N. To do this it is sufficient to show that the mapping f is bicontinuous, since the fact that the mapping is one-to-one follows from the isomorphism for abstract groups.

Let $a^* \subset G^*$, and $f(a^*) = A$. Let us denote by U^* a neighborhood of the element A in the space G/N. By Definition 24, U^* is composed of all cosets of the form Nx, where $x \varepsilon U$, and U is some fixed neighborhood in the space G. Let a be an element of U such that $A = Na$. Since the mapping g is open and $g(a) = a^*$, there exists a neighborhood V^* of the element a^* such that $g(U) \supset V^*$. It follows from this that $f(V^*) \subset U^*$. For let $x^* \varepsilon V^*$. Then there exists an element $x \varepsilon U$ such that $g(x) = x^*$. Hence $f(x^*) = Nx \varepsilon U^*$, and the mapping f is continuous.

Let us now denote by f^{-1} the mapping inverse to f. Let $A = Na \varepsilon G/N$ and $f^{-1}(A) = a^*$. Also let U^* be a neighborhood of the element a^*. Since the mapping g is continuous and $g(a) = a^*$, it follows that there exists a neighborhood V of the element a such that $g(V) \subset U^*$. We denote by V^* the neighbor-

hood of the element A which is composed of all cosets of the form Nx, where $x \in V$. Since $g(V) \subset U^*$, it follows that $f^{-1}(V^*) \subset U^*$. Hence the mapping f^{-1} is continuous.

We see thus that the mapping f is isomorphic for abstract groups, and bicontinuous for topological spaces. Therefore, f is an isomorphic mapping of the topological group G^* on the topological group G/N.

It is worth noting that if the mapping g were not open, it would have been possible to prove only the continuity of f^{-1}, but not the continuity of f.

If we restrict ourselves, however, to the consideration of locally compact groups satisfying the second axiom of countability, then for such groups every homomorphism will be open.

THEOREM 13. *If G and G^* are two locally compact topological groups satisfying the second axiom of countability, then every homomorphic mapping g of the group G on the group G^* is open.*

PROOF. Let W be an open set of the space G. We shall show that $g(W)$ contains an open set.

Since the topological space G is locally compact and regular (see §16, F)), there exists an open set V such that its closure $\overline{V}$ is compact and $\overline{V} \subset W$. The set of all the open sets of the form Vx covers the whole space G, and since the space G satisfies the second axiom of countability it follows that from this covering we can select a countable covering (see §12, H)). Hence there exists a countable sequence of points a_n, $n = 1, 2, \cdots$, such that the system of open sets Va_n, $n = 1, 2, \cdots$, covers the space G. Suppose that $g(\overline{V}a_n) = F_n$. Since $\overline{V}a_n$ is compact, F_n is also compact (see Theorem 8). Since G^* is regular and satisfies the second axiom of countability, F_n is closed (see §13, B)). The system of sets F_n, $n = 1, 2, \cdots$, covers the space G^*.

We now show that among the sets F_n there exists at least one containing an open set. Let us suppose the contrary to be true. Let V^* be an open set of G^* such that its closure $\overline{V}^*$ is compact. Since F_1 does not contain an open set, there exists a point $b_1 \in V^*$ not belonging to F_1. There exists further a neighborhood V_1 of the point b_1 such that $\overline{V}_1 \in V^*$, and $\overline{V}_1$ does not intersect F_1. In the open set V_1 we can also find a point b_2 not belonging to F_2, and a neighborhood V_2 such that $\overline{V}_2 \subset V_1$ and $\overline{V}_2$ does not intersect F_2. Continuing this process we construct a sequence of open sets V_n, $n = 1, 2, \cdots$, such that $\overline{V}_{n+1} \subset V_n$, $\overline{V}_n$ is compact and does not intersect F_n. By Theorem 6 the intersection of all the sets $\overline{V}_n$, $n = 1, 2, \cdots$, is not empty, i.e., there exists a point b not belonging to any of the sets F_n. This is however impossible, since the system F_n, $n = 1, 2, \cdots$, covers the space G^*. Hence one of the sets F_n, say F_k, contains an open set, but then the set $g(\overline{V}) = F_k g(a_k^{-1})$ also contains an open set (see §16, C)). Since $\overline{V} \subset W$, $g(W)$ contains an open set.

Let U be a neighborhood of the identity $e \in G$. Then there exists a neighborhood W of the identity such that $WW^{-1} \subset U$ (see §16, A)). From what we have just proved $g(W)$ contains an open set W^*. Let $q \in W^*$ and let p be a

point of W such that $g(p) = q$. Then Wp^{-1} is a neighborhood of the point e which is contained in U. For since $p \varepsilon W$, $Wp^{-1} \subset WW^{-1} \subset U$. Also W^*q^{-1} is a neighborhood of the identity $e^* \varepsilon G^*$. Since $g(W) \supset W^*$, it follows that $g(Wp^{-1}) \supset W^*q^{-1}$, and therefore, $g(U) \supset W^*q^{-1}$. Hence the mapping g is open (see B)).

D) We note that if an open homomorphic mapping g of a topological group G on a topological group G^* has a kernel containing only the identity, then this mapping is isomorphic.

In fact, under these conditions the homomorphism g is one-to-one and coincides with the natural isomorphism of the groups G/N and G^*, as constructed in Theorem 12.

E) Let G and G^* be two topological groups, and let f be an open homomorphic mapping of the group G on the group G^* with the kernel N'. Then there exists a one-to-one correspondence between the subgroups of the group G^* and the subgroups of the group G which contain N'. This correspondence can be established as follows: if N^* is a subgroup of the group G^*, then the corresponding subgroup N of the group G is determined as the complete inverse image $N = f^{-1}(N^*)$ of the group N^* under the mapping f. If N is a subgroup of the group G containing N', then the corresponding subgroup N^* is determined as the image $N^* = f(N)$ of the group N under the mapping f. The two relations thus established are inverses of each other. Moreover, the normal subgroups correspond to each other, and if N and N^* are two corresponding normal subgroups then the factor groups G/N and G^*/N^* are isomorphic.

We shall first discuss the mapping of N^* on N.

The set N, being a complete inverse image of the set N^*, is closed and contains N'. Moreover N is a subgroup of the abstract group G (see §3, G)), and therefore N is a subgroup of the topological group G as well. If N^* is a normal subgroup of the group G^*, we denote by g the natural homomorphic mapping of the group G^* on the group $G^*/N^* = G^{**}$. Then $h(x) = g(f(x))$ is an open homomorphic mapping of the group G on the group G^{**} with kernel N. It therefore follows from Theorem 12 that N is a normal subgroup of the group G, and that the factor groups G/N and G^*/N^* are isomorphic with each other.

We now consider the mapping of N on N^*, where $N^* = f(N)$, and $N \supset N'$. We shall first show that the complete inverse image of the set N^* in the group G, under the mapping f coincides with N. In fact if $f(a) \varepsilon N^*$, there exists an element $b \varepsilon N$ such that $f(a) = f(b)$. Then $f(ab^{-1}) = e^*$, i.e., $ab^{-1} \varepsilon N' \subset N$, or $a \varepsilon Nb = N$. It follows from this that $f(G - N) = G^* - N^*$, and since the mapping f is open and $G - N$ is an open set $G^* - N^*$ is also an open set, i.e., N^* is closed in G^*. The fact that N^* is a subgroup or a normal subgroup of the abstract group G^* can be proved directly (see §3, F)).

Example 28. Let G be the additive group of real numbers with the discrete topology, and G^* the additive group of real numbers with its natural topology. We shall associate with every real number $x \varepsilon G$ the same real number $x^* \varepsilon G^*$, and write $g(x) = x^*$. It is obvious that the mapping g is a homomorphic

mapping of the group G on the group G^*. Algebraically g is even isomorphic, but g is not an open mapping, and therefore not isomorphic for the topological groups G and G^*. For, every element x of the group G forms an open set, but this is not true for the corresponding element x^*. Theorem 13 does not hold in this case because the group G does not satisfy the second axiom of countability.

Example 29. Let G be a plane given in cartesian coordinates. Its points, or equivalently, its vectors, form an additive topological group. Let H be a straight line in the plane G passing through the origin and having the slope α. It is obvious that H is a subgroup of the topological group G. Let us denote by N the totality of all points in the plane G with integral coordinates. Then N is also a subgroup of the group G. Let $G^* = G/N$, and let us denote by g the natural homomorphic mapping of the group G on the group G^* (see C)). Under this homomorphism g the subgroup H goes into a subgroup H^* of the abstract group G^* (see §3, F)). However, H^* may not be a closed subset of the topological space G^*. It is easy to verify that H^* is a closed set if α is a rational number; as a matter of fact H^* is a closed curve in G^* in this case. If α is irrational, H^* forms a set everywhere dense in G^*.

In order to give a complete proof of this fact we need a result to be stated later in Example 51. It is easy to see that if α is irrational, there exists a number β such that β and $\alpha\beta$ are linearly independent, i.e., the relation $p\beta + q\alpha\beta = r$, where p, q, and r are integers implies $p = q = r = 0$. Let us now denote by a an element of G with coordinates β and $\alpha\beta$, and by A a subgroup having a for a generator. Then $A \subset H$; moreover, it follows from the result stated in Example 51 that $g(A)$ is everywhere dense in G^*. Hence H^* is also everywhere dense in G^*.

We see, therefore, that if α is irrational, H^* need not be closed. Hence H^* is not a subgroup of the topological group G^*, but is nevertheless a topological group (see §18, A)). The mapping g of the topological group H on the topological group H^* is homomorphic, but this homomorphism is not open. Algebraically the mapping g of the group H on the group H^* is even isomorphic. It can be readily checked that although H^* satisfies the second axiom of countability, (see §12, B)) it is not locally compact. This explains why Theorem 13 does not hold here. The abstract groups H and H^* are isomorphic, but the topological groups H and H^* are not isomorphic. They are not even homeomorphic, since only one of them is locally compact.

20. The Intersection and Product of Subgroups. Direct Product

In this section we generalize to topological groups the concepts and results which were established for abstract groups in §5.

A) Let G be a topological group and M a set of its subgroups. Let us denote by D the intersection of all subgroups belonging to M. Then D is a subgroup of the group G. If all the subgroups of M are normal subgroups of G, then D is also a normal subgroup of G.

In §5 we showed that D is a subgroup or a normal subgroup of the abstract group G (see §5, A)). It was shown in §7 that the intersection of an arbitrary number of closed subsets of a topological space is a closed subset of that space (see §7, E)). Hence D is respectively a subgroup or a normal subgroup of the topological group G.

B) Let A be a set of elements of the topological group G. Then there exists a unique minimal subgroup of the group G containing A. In the same way there exists a unique minimal normal subgroup of the group G which contains the set A.

Let us denote by M the set of all subgroups of the group G which contain A. The intersection D of all the subgroups belonging to M is a subgroup of the topological group G, by A). Obviously D is the minimal subgroup containing A. Similarly we can demonstrate the existence of the minimal normal subgroup of the group G containing A.

C) If H is a subgroup and N a normal subgroup of a topological group G then the intersection $H \cap N = D$ is a normal subgroup of the topological group H (see §18, A)).

We have shown in §5, that D is a normal subgroup of the abstract group H (see §5, C)). At the same time D is a closed subset of the space G and, therefore, also of the space H (see §10, A)). Hence D is a normal subgroup of the topological group H.

D) Let H be a subgroup and N a normal subgroup of the topological group G. Suppose that the product HN is a closed subset of the topological space G. Then $HN = NH$ is a subgroup of the topological group G. If, moreover, H is a normal subgroup of the topological group G, then HN is also a normal subgroup. Obviously, the condition of closure of the set HN is always satisfied by a compact topological group G satisfying the second axiom of countability. We note that if G satisfies the second axiom of countability than the compactness of one of the groups H or N is sufficient for the closure of HN.

We have shown in §5 that HN is a subgroup or a normal subgroup of the group G respectively (see §5, D)). Since we impose on HN the condition of closure it becomes a subgroup or a normal subgroup of the topological group G. We shall show now that if G satisfies the second axiom of countability, and if one of the groups H or N, say H, is compact, then the set HN is closed. Let $c_1, \cdots, c_n, \cdots$ be a sequence of elements of HN which converges to c. We have $c_n = a_n b_n$, where $a_n \in H$, $b_n \in N$, $n = 1, 2, \cdots$. Since H is compact, we can select from the sequence $a_1, \cdots, a_n, \cdots$ a subsequence $a_{n_1}, \cdots, a_{n_i} \cdots$ which converges to an element $a \in H$. We conclude from the convergence of the sequences $c_{n_1}, \cdots, c_{n_i}, \cdots$ and $a_{n_1}, \cdots, a_{n_i}, \cdots$ that the sequence $b_{n_1}, \cdots, b_{n_i}, \cdots$ converges to the element $a^{-1}c$, which belongs to N, since N is closed. Hence $c = a(a^{-1}c) \in HN$ and the closure of the set HN is established.

E) If $N_1, \cdots, N_k$ are normal subgroups of a topological group G, and if the

product $P = N_1 \cdots N_k$ is closed in G, then P is a normal subgroup of the topological group G.

It was shown in §5 that P is a normal subgroup of the abstract group G (see §5, E)); since moreover, P is closed in G, proposition E) is proved.

THEOREM 14. *Let H be a subgroup and N a normal subgroup of a locally compact topological group G satisfying the second axiom of countability. Suppose that the product $HN = P$ is a closed subset of the topological space G, and denote by D the intersection $H \cap N$. Then the factor group H/D is isomorphic with the factor group P/N* (see C), D)).

PROOF. In proving Theorem 2 we have shown that every element X of the group H/D is contained in a definite element X' of the group P/N. Let $f(X) = X'$. If $X = Dx$, where $x \varepsilon H$, then $X' = Nx$. As was shown in Theorem 2, the mapping f of the abstract group H/D on the abstract group P/N is isomorphic. We shall show that f is at the same time a bicontinuous mapping of the space H/D on the space P/N.

Let U'^* be a neighborhood of the element A' in the space P/N. By Definition 24, U'^* is composed of all cosets of the form Nx, where $x \varepsilon U'$, and U' is a definite neighborhood in the space P. The product NU' is an open set in P which contains A'. Therefore the intersection $H \cap (NU') = U$ is an open set in H (see §10, B)), containing $A = f^{-1}(A')$, since $A \subset A'$. We denote by U^* the neighborhood of the element A composed of all cosets of the form Dx, where $x \varepsilon U$. It is obvious that if $X \varepsilon U^*$, then $f(X) \varepsilon U'^*$. Hence the mapping f is continuous.

In this way the mapping f is algebraically isomorphic and topologically continuous, and therefore f is a homomorphic mapping of the topological group H/D on the topological group P/N. It follows from Theorem 13 that f is an open mapping, and hence (see §19, D)) f is isomorphic. We can apply Theorem 13 here because the groups P and H are locally compact and satisfy the second axiom of countability (see §18, B), and §12, B)) and therefore the groups P/N and H/D are also locally compact and satisfy the second axiom of countability (see §18, E) and D)).

It is worth noting that Theorem 14 does not hold for general topological groups, as will be shown by an example.

DEFINITION 28. Let K and N be two normal subgroups of the topological group G. We say that G is *decomposed into the direct product* of its subgroups K and N if $KN = G$ and $K \cap N = \{e\}$.

DEFINITION 28′. Let K and N be two topological groups.. We denote by G the set of all pairs of elements (x, y) where $x \varepsilon K$, $y \varepsilon N$. Then G, being the direct product of the abstract groups H and K, is an abstract group (see Definition 10′). Similarly G is a topological space, being the topological product of the spaces K and N (see Definition 21). The topological group G thus constructed is called the *direct product* of the topological groups K and N.

This definition can be extended in an obvious manner to any finite number of topological groups.

We shall show that Definition 28′ actually defines a topological group. To do this it is sufficient to show that the group operations of the abstract group G are continuous in the topological space G. Let $a = (a', a'')$ and $b = (b', b'')$ be two elements of G. Let $c = ab^{-1} = (a'b'^{-1}, a''b''^{-1}) = (c', c'')$ and let us denote by W a neighborhood of the element c in the space G. By Definition 21, W is composed of all pairs of the form (z', z''), where $z' \varepsilon W'$, and $z'' \varepsilon W''$, and W' is a neighborhood of the element c' in the space K, while W'' is a neighborhood of the element c'' in the space N, $c' \varepsilon W'$, $c'' \varepsilon W''$. Because the group operations are continuous in the groups K and N, there exist neighborhoods U', V', U'', V'' of the elements a', b', a'', b'' such that $U'V'^{-1} \subset W'$, $U''V''^{-1} \subset W''$. Let us denote by U the set of all pairs (x', x'') such that $x' \varepsilon U'$, $x'' \varepsilon U''$, and by V the set of all pairs (y', y'') such that $y' \varepsilon V'$, $y'' \varepsilon V''$. Obviously U and V are neighborhoods of the elements a and b such that $UV^{-1} \subset W$. Hence G is actually a topological group.

Propositions F) and H) of §5 can be automatically extended to topological groups.

In order to establish the equivalence of Definition 28 and 28′, there remains to be proved the following proposition, which is, by the way, not true for general topological groups.

F) Let G be a locally compact topological group satisfying the second axiom of countability. Suppose that G is decomposed into the direct product of K and N, and denote by K' a topological group isomorphic with K, and by N' a topological group isomorphic with N. If G' is the direct product of the groups K' and N', then the topological groups G and G' are isomorphic.

Let f be an isomorphic mapping of the topological group K' on the topological group K, and g an isomorphic mapping of N' on N. To every element $(x, y) \varepsilon G'$ corresponds an element $h((x, y)) = f(x)g(y)$ of the group G. It was shown in §5 that h is an isomorphic mapping of the abstract group G' on the abstract group G (see §5, G)). We shall show that h is a continuous mapping of the space G' on the space G.

Let W be a neighborhood of the element $c = ab \varepsilon G$, where $a \varepsilon K$, $b \varepsilon N$. There exist neighborhoods U^* and V^* of the elements a and b in the space G such that $U^*V^* \subset W$. Suppose $U = K \cap U^*$, $V = N \cap V^*$. Then U and V are neighborhoods of the elements a and b in the spaces K and N (see §10, C)). Let us further suppose that $a' = f^{-1}(a)$, $b' = g^{-1}(b)$. Then there exist neighborhoods U' and V' of the elements a' and b' such that $f(U') \subset U$, $g(V') \subset V$. We denote by W' the neighborhood of the element (a', b') composed of all pairs (x, y) where $x \varepsilon U'$ and $y \varepsilon V'$. Obviously $h(W') \subset W$, and hence the mapping h is continuous.

Since the mapping h is algebraically isomorphic and topologically continuous, it follows from Theorem 13 that it is open, and therefore by remark D) of §19, h is an isomorphism. Theorem 13 is applicable because the groups K and

N are locally compact and satisfy the second axiom of countability (see §18, B) and §12, B)), and therefore the group G' is also locally compact and satisfies the second axiom of countability (see §15, F), and C)). We recall in passing that the space of a topological group is always regular (see §16, F)).

G) Let G be a locally compact topological group satisfying the second axiom of countability. If G is decomposed into the direct product of its subgroups K and N then K is isomorphic with the factor group G/N.

This proposition follows from Theorem 14.

Example 30. Let G be a plane given in cartesian coordinates. Its points form an additive topological group. We denote by N a straight line of slope α, and by H the set of all points having integral coordinates. H and N are normal subgroups of G. We further denote by P the product HN, i.e., the set of all elements of the form $h + n$, where $h \varepsilon H$, $n \varepsilon N$. P is closed in G if α is a rational number; for an irrational α, however, P is neither closed nor locally compact.

Let us discuss the case of irrational α. P is a topological group although it is not a subgroup of the topological group G (see §18, A)). The intersection $D = H \cap N$ contains zero only. It is obvious, however, that the groups H/D and P/N are not isomorphic, as the first is discrete, while the second is not discrete. We note further that the group P decomposes into the direct sum of its subgroups H and N, but the propositions F) and G) do not hold here.

21. Infinite Direct Product

In the theory of topological groups a special part is played by the infinite direct product, whose construction differs from the corresponding construction in the theory of abstract groups because of the possibility of passing to the limit.

Definition 29. Let G be a compact topological group satisfying the second axiom of countability, and M a countable set of normal subgroups of the group G, $M = \{G_1, \cdots, G_n, \cdots\}$. We say that the group G *decomposes into the direct product of the set M of its subgroups* if the following conditions are fulfilled:

1) The minimal normal subgroup of the group G (see §20, B)) which contains all the subgroups of the set M coincides with G.

2) If we denote by H_n the minimal normal subgroup of the group G which contains all the subgroups of the set M with the exception of G_n, then the intersection of all the groups H_n, $n = 1, 2, \cdots$, contains only the identity e of the group G.

A) The group G can be decomposed into the product of two of its subgroups G_n and H_n (see Definition 28 and 29).

The product G_nH_n is compact (see §15, E)) and hence is closed in G (see §13, B)). Hence G_nH_n is a normal subgroup of the group G (see §20, D)). Also G_nH_n contains the subgroups of the set M and hence by condition 1) $G_nH_n = G$. We denote by G_n' the intersection of all the groups H_k, $k = 1, 2, \cdots$, with the exception of the group H_n. Obviously $G_n \subset G_n'$. It

follows from condition 2) of Definition 29 that the intersection $G'_n \cap H_n = \{e\}$. Hence the intersection $G_n \cap H_n = \{e\}$, and G decomposes into the direct product of G_n and H_n.

B) For $i \neq j$ every element of the group G_i commutes with every element of the group G_j. Let $x_1, \cdots, x_n, \cdots$ be a sequence of elements of the group G such that $x_i \in G_i$, $i = 1, 2, \cdots$. Then the infinite product $x_1 \cdots x_n \cdots$ converges, and every element of the group G is uniquely represented in the form of a product.

Since $G_i \subset H_j$, the commutativity of the elements of the groups G_i and G_j follows from A) (see §5, F)).

We suppose that $y_m = x_1 \cdots x_m$, and show that the sequence y_m, $m = 1, 2, \cdots$, converges. Since the intersection of all the sets H_n contains only the identity, there exists for every neighborhood V of the identity a number t which is such that $H_1 \cap \cdots \cap H_t \subset V$ (see §13, C)). It follows from this that for $p > t$ and $q > t$ we have $y_q y_p^{-1} \subset V$. Since G is compact, the sequence y_m, $m = 1, 2, \cdots$, has at least one limit point x. Suppose that there is another limit point x' of the same sequence. Denote by U and U' neighborhoods of x and x' whose closures do not intersect (see §12, A)). Then $\overline{U}'\overline{U}^{-1}$ is a compact set not containing the identity, and therefore there exists a neighborhood V of the identity such that V does not intersect $\overline{U}'\overline{U}^{-1}$. Since x and x' are limit points of the sequence y_m, $m = 1, 2, \cdots$, there exist number $p > t$ and $q > t$ such that $y_p \in U$, $y_q \in U'$; but then $y_q y_p^{-1}$ is not contained in V contrary to what has been shown above. Hence $x = x'$.

We note that the infinite product $x_1 \cdots x_n \cdots$ in which $x_k = e$ belongs to H_k.

Let x now be an arbitrary element of the group G. Since G decomposes into the direct product of the subgroups G_n and H_n, it follows that $x = x_n z_n$, where $x_n \in G_n$, $z_n \in H_n$ (see §5, F)). We form the infinite product $x_1 \cdots x_n \cdots = x'$ and show that $x = x'$. We have $x'x^{-1} = x_1 \cdots x_n \cdots x_n^{-1} z_n^{-1} \subset H_n$. Since the number n is arbitrary $x'x^{-1}$ belongs to the intersection of all the H_n, and therefore by condition 2) of Definition 29, $x'x^{-1} = e$.

Let us now suppose that the same element x is represented in two ways as an infinite product of the type under consideration. We should then have

$$x = x_1 \cdots x_n \cdots = x'_1 \cdots x'_n \cdots$$

from which it would follow that

$$x'^{-1}_n x'_1 \cdots x'_n \cdots x_n x_1^{-1} \cdots x_n^{-1} \cdots = x'^{-1}_n x_n.$$

But the left side of this last equation belongs to H_n, while the right side belongs to G_n, hence $x'^{-1}_n x_n = e$, i.e., $x_n = x'_n$ for every n.

Definition 29′. Let M be a countable set of compact topological groups satisfying the second axiom of countability, $M = \{G_1, \cdots, G_n, \cdots\}$. We construct from the groups of the set M a new topological group G which is

also compact and satisfies the second axiom of countability, and which we shall call the *direct product* of the groups belonging to the set M. The elements of the set G will be all the sequences $x = \{x_1, \cdots, x_n, \cdots\}$, where $x_n \in G_n$, $n = 1, 2, \cdots$. The product of two elements x, y of the group G, where $y = \{y_1, \cdots, y_n, \cdots\}$, is given by the formula

$$xy = \{x_1y_1, \cdots, x_ny_n, \cdots\}.$$

The neighborhoods in the space G are defined as follows: let $U_1, \cdots, U_r$ be a set of neighborhoods in the spaces $G_1, \cdots, G_r$. Then the neighborhood U of the space G is composed of all the elements $x = \{x_1, \cdots, x_n, \cdots\}$ such that $x_i \in U_i$, $i = 1, 2, \cdots, r$. The totality of all sets of the type U gives a complete system of neighborhoods of the space G.

It is not hard to see that the group G thus obtained does not depend on the way in which the groups of the set M are numbered.

The identity of the group G is $e = \{e_1, \cdots, e_n, \cdots\}$, where e_i is the identity of the group G_i, $i = 1, 2, \cdots$. The inverse of the element $x = \{x_1, \cdots, x_n, \cdots\}$ is the element $x^{-1} = \{x^{-1}, \cdots, x_n^{-1}, \cdots\}$. It follows readily that all the group axioms are satisfied in the set G.

We shall show that the complete system of neighborhoods given in Definition 29′ satisfies the conditions of Theorem 3. Let x and y be two distinct elements of the group G. Since $x \neq y$ there exists a number k such that $x_k \neq y_k$. Let U'_k be a neighborhood of the element x_k not containing the element y_k. We define the neighborhood U of the element x by letting $U_1 = G_1, \cdots, U_{k-1} = G_{k-1}$, $U_k = U'_k$. Obviously U does not contain the element y.

Let U and V be two neighborhoods of the element x. Let U be determined by the system of neighborhoods $U_1, \cdots, U_r$, and V by the system of neighborhoods $V_1, \cdots, V_s$. If $r < s$, we suppose that $U_{r+1} = G_{r+1}, \cdots, U_s = G_s$. There exists a neighborhood W_i of the element x_i which is contained in the intersection $U_i \cap V_i$, $i = 1, \cdots, s$. Then the neighborhood W of the element x defined by the sequence of neighborhoods $W_1, \cdots, W_s$ obviously possesses the property $W \subset U \cap V$.

The condition of continuity of the group operations in G can be verified easily as was done in §20 for the direct product of two topological groups.

The fact that the second axiom of countability is satisfied in G follows from the construction of the complete system of neighborhoods in G, since we obtain only a countable system of neighborhoods.

We shall now show that the space G is compact. Let $x_k = \{x_{1k}, \cdots, x_{nk}, \cdots\}$, $k = 1, 2, \cdots$, be a sequence of elements of the space G. We make use of the diagonal process to select from this sequence a converging subsequence. By Theorem 9 there exists an increasing sequence $k(1), \cdots, k(i)$ of natural numbers such that the sequence $x_{nk(i)}$, $i = 1, 2, \cdots$, of elements of the group G_n converges in G_n to the element y_n. It is readily seen that the element $y = \{y_1, \cdots, y_n, \cdots\}$ is a limit element for the sequence $x_{k(i)}$, $i = 1, 2, \cdots$, in the group G. For if U is a neighborhood of the element y defined by the sys-

tem of neighborhoods $U_1, \cdots, U_r$, then beginning with some number j (i.e., for $i > j$) we have $x_{rk(i)} \varepsilon U_n$, $n = 1, \cdots, r$, i.e., $x_{k(i)} \varepsilon U$ for $i > j$. We have in this way selected a convergent subsequence from an arbitrary sequence, and hence G is compact.

G) Let M be a countable set of compact topological groups satisfying the second axiom of countability, $M = \{G_1, \cdots, G_n, \cdots\}$, and G the direct product of the groups belonging to M (see Definition 29′). We denote by G'_k the set of all elements $x = \{x_1, \cdots, x_n, \cdots\}$ such that $x_i = e_i$ for $i \neq k$, where e_i is the identity of the group G_i. Then every set G'_k is a normal subgroup of the group G, and G is decomposed into the direct product of the subgroups G'_k, $k = 1, 2, \cdots$.

Let $x = \{x_1, \cdots, x_n, \cdots\}$ be an arbitrary element of the group G. Letting $y_m = \{x_1, \cdots, x_m, e_{m+1}, e_{m+2}, \cdots\}$, it is easy to see that the sequence y_m, $m = 1, 2, \cdots$, converges to x, for every neighborhood of the element x contains all elements y_m if m is sufficiently large.

We denote by H'_k the set of all elements $x = \{x_1, \cdots, x_n, \cdots\}$ such that $x_k = e_k$. H'_k can be regarded as the direct product of all the groups of the set M with the exception of the group G_k, in place of which is taken the group $\{e_k\}$. It follows that H'_k is compact, and being a subset of the space G, is closed. We can also check that H'_k is a normal subgroup of the group G, that $G'_i \subset H'_k$ for $i \neq k$, and that H'_k is the minimal normal subgroup containing all the groups G'_n with the exception of the group G'_k. For such minimal normal subgroup must contain all products of the form $G'_1, \cdots, G'_m$ which do not contain G'_k, and because of closure it must contain all the limit elements, i.e., all the elements belonging to H'_k. Obviously the intersection of all the subgroups H'_n contains only the identity of the group G.

We can also verify that G'_k is a normal subgroup of the group G, and in the same way as was done for H'_k convince ourselves that the minimal normal subgroup containing all the subgroups G'_n coincides with G.

D) Let G be a compact topological group satisfying the second axiom of countability. Suppose that G is decomposed into the direct product of a countable set M of its subgroups, $M = \{G_1, \cdots, G_n, \cdots\}$. Let G'_k be a group isomorphic with the group G_k, $k = 1, 2, \cdots$. If we denote by G' the direct product of the groups $G'_1, \cdots, G'_n, \cdots$, then the groups G' and G are isomorphic.

I do not give here the proof of this fact because it is similar to the proof of the analogous fact given in a preceding section (see §20, F)).

Example 31. Let M be a countable set of finite abstract groups. We shall consider each of the groups of M as a topological group with the discrete topology. Then all the groups of the set M are compact and satisfy the second axiom of countability. We denote by G the direct product of all groups of the set M. The group G is compact and satisfies the second axiom of countability, while except for trivial cases G contains infinitely many elements. Hence G has a non-discrete topology. We have here a method for constructing topolog-

ically non-trivial groups from abstract groups. However, as will be shown later (see Example 33) this method gives only topological groups of a special type, namely 0-dimensional groups, and does not even give all such groups

EXAMPLE 32. We can define the direct product of a non-countable number of groups of the set M just as was done in Definition 29′. We denote the groups of the set M by G_α, where α is the index of some, in general, non-countable set. The elements x of the direct product G are defined as the sets of elements x_α, where $x_\alpha \varepsilon G_\alpha$, and where one element x_α has been taken from each group G_α. We shall call the elements x_α the *coordinates* of the element x. The product of two elements x and y of G we define as before, i.e., we set $(xy)_\alpha = x_\alpha y_\alpha$. In order to define a neighborhood in G we take a finite system of indices $\alpha_1, \cdots, \alpha_r$, a system of neighborhoods $U_{\alpha_1}, \cdots, U_{\alpha_r}$ in the spaces $G_{\alpha_1}, \cdots, G_{\alpha_r}$, and then define the corresponding neighborhood U of the space G as the set of all elements x for which $x_{\alpha_i} \varepsilon U_{\alpha_i}$, $i = 1, 2, \cdots, r$.

Let us consider the set H in G of all the elements x having at most a countable set of coordinates distinct from the identities. It is easily seen that H is compact and forms a group. At the same time the closure of the set H coincides with G. It does not follow from this, however, that $H = G$. This would have been true if G had satisfied the second axiom of countability. But if the groups of the set M are non-trivial, that is if each one contains more than a single element, and if M has more than a countable number of elements, then H is obviously distinct from G. It follows from this that G does not satisfy the second axiom of countability. It is worth noting that although H is compact it is not a closed subset of the space G.

The following interesting condition known as *bicompactness* is satisfied by the group G constructed above, namely that from any covering of the space G by open sets a finite covering can be selected. This fact, however, cannot be proved easily, and we shall not stop to consider it here. We only remark that bicompactness is in general more restrictive than compactness, but if the second axiom of countability is satisfied, compactness and bicompactness coincide.

22. Connected and 0-dimensional Groups

In this section we shall consider some rather special topological properties of topological groups which have no analogues in abstract groups.

A) Let G be a topological group, and let N be the component of the point e in the topological space G (see §11, D)). Then N is a normal subgroup of the group G.

Let a and b be two elements of N. Since N is connected it follows that the set aN^{-1} is also connected (see §16, B)). Moreover aN^{-1} contains e. Hence $aN^{-1} \subset N$, and we have $ab^{-1} \varepsilon N$, i.e., N is a subgroup of the abstract group G. Since N is closed in G (see §11, D)), N is a subgroup of the topological group G. If x is an arbitrary element of G, then $x^{-1}Nx$ is a connected set containing the identity e, and hence $x^{-1}Nx \subset N$, and N is a normal subgroup of the topological group G.

B) In case the space of the topological group G is connected, the component of the identity of the group G coincides with G, and the group itself is said to be *connected*. If, on the other hand, the component of the identity of the group G contains only the identity, the group G is called a *0-dimensional* or *totally-disconnected* group.

C) Let G be a topological group and N the component of the identity in G. Then the factor group $G/N = G^*$ is a 0-dimensional group.

Let f be the natural homomorphic mapping of the group G on the group G^* (see §19, C)). The mapping f is an open homomorphic mapping of the group G on the group G^*. Let us denote by P^* the component of the identity of the group G^*, and by P the complete inverse image of the set P^* under the mapping $f, f^{-1}(P^*) = P$. We shall show that the mapping f of the space P on the space P^* is open. Let U be an open set of the space P. Then there exists a neighborhood V in the space G such that $U = P \cap V$ (see §10, B)). It can be seen readily that $f(U) = P^* \cap f(V)$. But since f is an open mapping of the group G on the group G^*, it follows that $f(V)$ is an open set in G^*, and hence $f(U)$ is an open set of the space P^*.

Let us now suppose that G^* is not a 0-dimensional group, that is, that P^* contains elements different from the identity. Then N is a part of the space P and hence P is not connected. Therefore, P can be decomposed into the sum of two non-intersecting sets A and B, each of which is non-empty, and is an open set in the space P (see §11, A)). It is not hard to see that if $a \in A$, then $Na \subset A$, for if Na were to intersect B, it would decompose into two non-intersecting closed sets, but, in reality, Na is connected when N is. It follows therefore that the sets $f(A)$ and $f(B)$ do not intersect. But these sets are open in the space P^*, and therefore P^* decomposes into two non-intersecting subsets which are open sets in the space P^*, which is impossible, since P^* is connected.

We now take up some properties of connected groups.

THEOREM 15. *A connected topological group G is generated by an arbitrary neighborhood U of the identity. This means that G coincides with the sum of all sets of the form U^n, $n = 1, 2, \cdots$, or, what is the same, that every element of G can be represented as a finite product of elements belonging to U.*

PROOF. Let V be the sum of all sets of the form U^n. Since all sets of the form U^n are open sets (see §16, C)), it follows that V is an open set. We shall show that V is at the same time a closed set. Let us suppose that a belongs to the closure of the set V, $a \in \overline{V}$. Since aU^{-1} is a neighborhood of the element a, it intersects V, i.e., there exists an element $b \in V$ such that $b \in aU^{-1}$. Since $b \in V$, there exists a number m such that $b \in U^m$, and hence $b = u_1 \cdots u_m$, where $u_i \in U$, $i = 1, \cdots, m$. Since $b \in aU^{-1}$, it follows that $b = au_{m+1}^{-1}$, where $u_{m+1} \in U$. We have therefore $a = u_1 \cdots u_m u_{m+1}$, where $u_j \in U$, $j = 1, \cdots, m, m + 1$. Hence $a \in U^{m+1} \subset V$, i.e., V is closed. Let $W = G - V$. Since V is closed and open, W is also closed and open. But if W were not empty, G would

decompose into the sum of two non-intersecting closed sets, which would contradict the assumption that the group G is connected; hence $G = V$.

D) We shall call the totality of all central elements of the abstract group G (see Definition 7), the *center* Z of the topological group G. Z is a normal subgroup of the topological group G. Every subgroup N of the group Z is also a normal subgroup of the group G and is called a *central normal subgroup*.

We have shown in §4 that Z is a normal subgroup of the abstract group G. We shall now show that Z is closed in G. Let $a \varepsilon \bar{Z}$, and let us suppose that there exists an element $x \varepsilon G$ such that $a' = x^{-1}ax \neq a$. Since the space G is regular (see §16, F)), there exist two neighborhoods U and U' of the elements a and a' whose closures do not intersect (see §12, A)). Let $V = Z \cap U$. It is easy to see that $a \varepsilon \bar{V}$, but then $a' = x^{-1}ax \varepsilon x^{-1}\bar{V}x = \overline{x^{-1}Vx} = \bar{V}$ (see §16, B)). But this is impossible since U' and $\bar{V}$ do not intersect. Hence $x^{-1}ax = a$ and $a \varepsilon Z$, i.e., $\bar{Z} = Z$.

Any subgroup N of the group Z, being closed in Z, must also be closed in G (see §10, A)). And since N is a normal subgroup of the abstract group G (see §4, B)), it must be a normal subgroup of the topological group G.

Theorem 16. *Every discrete normal subgroup N of a connected topological group G is a central normal subgroup of this group* (see §17, A)).

Proof. Since N is a discrete group, there exists for each element a of N a neighborhood V which contains no element of the group N except the element a itself. Since $e^{-1}ae = a$, there exists a neighborhood U of the identity such that $U^{-1}aU \subset V$ (see §16, A)). Let $u \varepsilon U$; then $u^{-1}au \varepsilon V$, but since N is a normal subgroup of the group G, it follows that $u^{-1}au \varepsilon N$, and hence $u^{-1}au = a$. If x is an element of G, then by Theorem 15, $x = u_1 \cdots u_n$, where $u_i \varepsilon U$, $i = 1, \cdots, n$. Since a commutes with every element u_i, a must commute with x, i.e., $x^{-1}ax = a$. Hence N belongs to the center Z of the group G and the theorem is proved.

Theorem 16 is important because it facilitates the process of finding discrete normal subgroups of connected topological groups, which play an important part in the theory of topological groups.

We now consider 0-dimensional groups, and limit ourselves to locally compact groups satisfying the second axiom of countability.

Theorem 17. *Let G be a locally compact topological 0-dimensional group satisfying the second axiom of countability. If U is a neighborhood of the identity of the group G, then there exists a subgroup H of the group G such that $H \subset U$ and H is an open set in G. Since H is an open set the space G/H is discrete* (see Definition 24).

Proof. Let $V_1, \cdots, V_n, \cdots$ be a basis about the identity e (see §8, B')) such that $V_{n+1} \subset V_n$, $n = 1, 2, \cdots$ (see §12, D)). Let M be a compact subset of the space G containing the identity e. We shall say that a point $a \varepsilon M$ can be *connected to e over the set M by a chain of order n*, if there exists a sequence

$a_1 = e, a_2, \cdots, a_k = a$ of points of M such that $a_i^{-1}a_{i+1} \in V_n$, $i = 1, \cdots, k-1$. Let us denote by M_n the totality of the points which can be connected to e by chains of order n over the set M. It can readily be seen that every point $a \in M_n$ can be connected to e by a chain of order n over the set M_n itself. Moreover $M_{n+1} \subset M_n$. We shall show that the set M_n is compact and is a relative open set in the space M (see §10, B)). Let $a \in M_n$. Then the intersection $aV_n \cap M$ lies entirely in M_n and is a relative neighborhood of the point a in the space M. Hence M_n is a relative neighborhood in the space M. Let a be a point of M not belonging to M_n; then aV_n^{-1} cannot intersect M_n, and therefore M_n is closed, and hence compact (see §13, A)).

We denote by M^* the intersection of all the sets M_n, $n = 1, 2, \cdots$, and show that M^* is connected. It will follow from this that M^* contains only the identity e, since by assumption the group G is a 0-dimensional group.

Suppose that M^* can be decomposed into the sum of two non-empty non-intersecting closed sets A and B, $e \in A$. The set $A^{-1}B$ is compact and does not contain the identity; therefore there exists a sufficiently large number r such that $V_r^2V_r^{-1}$ does not intersect $A^{-1}B$. We shall now show that if $b \in B$ we cannot connect b to e over the set M^*V_r by a chain of order r. First, it is clear that the sets AV_r and BV_r do not intersect; therefore if there exists a connecting chain it would have to have two adjacent points p and q such that $p \in AV_r$ and $q \in BV_r$, and therefore $p^{-1}q \in V_r^{-1}A^{-1}BV_r$. Since at the same time $p^{-1}q \in V_r$, it follows that $V_r^2V_r^{-1}$ intersects $A^{-1}B$. In this way we have arrived at a contradiction, and therefore it is impossible to connect the point b to e over the set M^*V_r by a chain of order r, and what is more, by a chain of order $s \geqq r$. Now let $s \geqq r$ be a sufficiently large number such that $M_s \subset M^*V_r$ (see §13, C)). Let $b \in B$; then since $b \in M_s$, b can be connected to e by a chain of order s over the set M_s; but this contradicts what we have just shown since $M_s \subset M^*V_r$.

Hence the intersection of all the sets M_n, $n = 1, 2, \cdots$, is connected and therefore contains only e.

Now let U be a given neighborhood of e. Without loss of generality we can suppose that its closure $\bar{U}$ is compact. Let us apply the above construction to the set $M = \bar{U}$. Let V be a neighborhood of the identity such that $V^2 \subset U$. Since the intersection of all the sets M_n, $n = 1, 2, \cdots$, contains only the identity there exists a sufficiently large number t such that $M_t \subset V$ (see §13, C)). Since M_t is a relative open set of the space $\bar{U}$, there exists an open set W of the space G such that $M_t = \bar{U} \cap W$ (see §10, B)). We have furthermore $U \cap W = M_t \subset V \subset V^2 \subset U$. Taking intersections with W on both sides of this relation we get $\bar{U} \cap W \subset U \cap W$. On the other hand $U \cap W \subset \bar{U} \cap W$ and hence $M_t = U \cap W$, i.e., M_t, being the intersection of two open sets U and W, is an open set in the space G. It can readily be seen, moreover, that every point $a \in M_t^2$ can be connected to the identity over the set M_t^2 by a chain of order t, and since $M_t^2 \subset U$, it follows that $M_t^2 \subset M_t$, and therefore we have for every natural number m that $M^m \subset M_t$, or for every $a \in M_t$, we have $a^m \in M_t$.

Since M_t is compact, the sequence $a, a^2, \cdots, a^m, \cdots$ has a limit point in M_t, from which it follows that for an arbitrary neighborhood V_n of the identity, there exist natural numbers m and $m' > m$ for which $a^{m'}(a^m)^{-1} = a^{m'-m} = a^{k_n} \subset V_n$. Let us denote by b a limit point of the sequence a^{k_n-1}, $n = 1, 2, \cdots$. We then have $ab = \lim_{n\to\infty} a^{k_n} = e$, and $b \in M_t$. Hence for every element $a \in M_t$ there exists an element $b \in M_t$ inverse to it, so that $M_t^{-1} \subset M_t$. It follows from remark B) of §2, that M_t is a subgroup of the abstract group G. Therefore $H = M_t \subset U$ is a compact open subgroup of the topological group G.

E) Let G be a compact topological 0-dimensional group satisfying the second axiom of countability. If U is a neighborhood of the identity of the group G, then there exists in G a normal subgroup N such that $N \subset U$ and N is an open set in G. Since the factor group G/N is both discrete and compact, it is finite.

Let H be a subgroup of the group G constructed as in Theorem 17. We denote by N the intersection of all the subgroups of the form $x^{-1}Hx$, where x is an arbitrary element of G. It follows from remark A) of §20 that N is a subgroup of the group G, and it can easily be seen that N is a normal subgroup of G. We shall show that N is an open set in G. To do this we show first of all that N contains a neighborhood of the identity. For if N contained no neighborhood of the identity there would exist a sequence a_i, $i = 1, 2, \cdots$, of elements not belonging to N which would converge to the identity e. Since $a_i \in G - N$, it follows that $a_i = x_i^{-1}b_ix_i$, where $b_i \in G - H$, $i = 1, 2, \cdots$. Since G is compact we can suppose without loss of generality that the sequences x_i and b_i, $i = 1, 2, \cdots$, converge to the elements x and b respectively. Since H is open, $b \in G - H$. Moreover, $x^{-1}bx = e$, or what is the same, $b = e$ but that is impossible since $b \in G - H$, and $e \in H$. Hence there exists a neighborhood V of the identity e which is entirely contained in N. Since N is a group we have $Vn \in N$ for any $n \in N$, and hence the subgroup N contains with every point n its neighborhood Vn, i.e., N is an open set.

F) We note that if a topological group G is a 0-dimensional group it has no connected subset containing more than a single element.

For if F is a connected subset of the group G which contains two distinct elements a and b, then the component of the identity e must contain the set Fa^{-1}, i.e., the element $ba^{-1} \neq e$ belongs to the component of the identity, and therefore G is not a 0-dimensional group.

The following trivial proposition G) is a variant of Theorem 17.

G) If every neighborhood U of the identity of the topological group G contains an open subgroup H of the group G, then G is a 0-dimensional group.

The group G decomposes into the sum of two non-intersecting open sets H and $G - H$. Hence the component of the identity of the group G, being connected, must belong to H, and hence to U; but since U is an arbitrary neighborhood of the identity, the component of the identity of the group G contains only the identity.

Example 33. Let us consider the direct product G given in Example 31 of a countable number of arbitrary groups G_n, $n = 1, 2, \cdots$. Let us denote

by C_k the set of all the elements $x = \{x_1, \cdots, x_n, \cdots\}$ such that $x_i = e_i$, $i = 1, \cdots, k$. It is not hard to see that C_k is a normal subgroup of the group G, and that the factor group G/C_k is isomorphic with the direct product of the groups $G_1, \cdots, G_k$. Hence the normal subgroup C_k is open in G since the factor group G/C_k is finite. We note further that for every neighborhood U of the identity of the group G there exists a number m such that $C_m \subset U$. From this it follows readily that the component of the identity of the group G contains only the identity (see G)). Hence G is a 0-dimensional group.

EXAMPLE 34. Let G be the additive group of real numbers. Then G is a topological group. Let us denote by H the set of all rational numbers. H is obviously a subgroup of the abstract group G, and therefore H is a topological group (see §18, A)). Obviously, the component of zero of the group H contains only zero. Hence H is 0-dimensional. It is worth noting, however, that the group H can be generated by any neighborhood whatever of zero (see Theorem 15). This shows that connected groups are not the only groups which enjoy the properties formulated in Theorem 15. We can conclude from this that G does not possess an open subgroup which is contained in U. Hence Theorem 17 does not hold for general 0-dimensional groups. The group H, although it satisfies the second axiom of countability, is nevertheless not locally compact.

23. Local Properties. Local Isomorphism

Of special importance for topological groups are the so-called *local properties*, i.e., those properties determined by the behavior of the group in the neighborhood of the identity. Local isomorphism is the most important of these properties.

DEFINITION 30. Two topological groups G and G' are called *locally isomorphic* if there exist neighborhoods U and U' of the identities e and e' and a homeomorphic mapping f of the neighborhood U on the neighborhood U' such that a) if the elements x, y, and xy belong to U, then $f(xy) = f(x)f(y)$; b) if the elements x', y' and $x'y'$ belong to U', then $f^{-1}(x', y') = f^{-1}(x')f^{-1}(y')$.

A) We note that if the above conditions are satisfied, the following conditions also hold: c) $f(e) = e'$, and d) if the elements x and x^{-1} belong to U, then $f(x^{-1}) = (f(x))^{-1}$.

In fact the elements e, e' and $ee = e$ belong to U, and hence $f(e) = f(e)f(e)$, from which it follows that $f(e) = e'$. Furthermore, if x and x^{-1} belong to U, then since $xx^{-1} = e \in U$, we obtain $e' = f(e) = f(x)f(x^{-1})$ i.e., $f(x^{-1}) = (f(x))^{-1}$.

B) We note that condition b) of Definition 30 follows from a). In fact if there exist neighborhoods U and U' satisfying condition a), then neighborhoods V and V' can be found satisfying both conditions a) and b).

Let V be a neighborhood of the identity such that $V^2 \subset U$. If we suppose that $V' = f(V)$, then condition a) is satisfied for both V and V'. Let us check condition b). Let the elements x', y' and $x'y'$ belong to V', and let $x = f^{-1}(x')$, $y = f^{-1}(y')$. Since x and y belong to V, we have $xy \in U$, and hence $f(xy)$

$= f(x)f(y) = x'y'$. It follows from this that $f^{-1}(x'y') = xy = f^{-1}(x')f^{-1}(y')$, i.e., condition b) is satisfied.

C) Let G be a topological group, and N a discrete normal subgroup. Then the groups G and $G/N = G'$ are locally isomorphic.

Let f be the natural homomorphic mapping of the group G on the group G' (see §19, C)). Let us denote by W a neighborhood of the identity of the group G which contains no element of the group N other than the identity. Let U be a neighborhood of G such that $UU^{-1} \subset W$, and let $f(U) = U'$. It can readily be seen that the mapping f is one-to-one between the open sets U and U'. In fact, let us suppose that the two elements x and y belonging to U go into the same element under the mapping f. Then $xy^{-1} \varepsilon N$, but $xy^{-1} \varepsilon W$ and hence $xy^{-1} = e$, or $x = y$. The mapping f is open and continuous (see §19, C)), and therefore it is bicontinuous on U. Condition a) of Definition 30 is satisfied for the mapping f because f is a homomorphic mapping. Therefore by remark B) condition b) is also satisfied, and the groups G and G' are locally isomorphic.

Proposition C) furnishes a method for constructing groups locally isomorphic to a given group. The following theorem shows that this method is rather general.*

THEOREM 18. *Let G and G' be two connected locally isomorphic topological groups. Then there exists a group H such that G is isomorphic to the factor group H/N and G' is isomorphic to the factor group H/N', where N and N' are two discrete normal subgroups of the group H.*

In proving this theorem we shall make use of the connectedness of the groups G and G', only in that they can both be generated by arbitrary neighborhoods of their identities (Theorem 15).

PROOF. Let U and U' be those neighborhoods of the identities of the groups G and G' for which the conditions of Definition 30 are satisfied, and let f be the corresponding mapping. Let us denote by K the direct product of the groups G and G' (see Definition 28′). Let V be the set of all the elements of the group K which can be represented in the form $(x, f(x))$, where $x \varepsilon U$. In order not to complicate the discussion let us suppose that the neighborhood U is symmetric, i.e., $U^{-1} = U$. We denote by H the sum of all the sets of the form V^n, $n = 1, 2, \cdots$. H may be defined equivalently as the totality of all the elements of the group K which can be represented as finite products of elements belonging to V. The set H is obviously a subgroup of the abstract group K, but it may not be a closed set in the topological space K. Nevertheless, from remark A) of §18, H forms a topological group in a natural way. We shall however introduce a topology into H by a different method.

Let U_α be a complete system of neighborhoods of the identity of the group G, where α is an index which, in general, runs over a non-countable set. Without loss of generality we may suppose that $U_\alpha \subset U$ for an arbitrary α. Let

* The proof of this theorem is due to B. A. Efrimovich.

$U'_\alpha = f(U_\alpha)$ and denote by V_α the set of all elements of the group K of the form $(y, f(y))$, where $y \in U_\alpha$. By remark C) of §17 the conditions of Theorem 10 are satisfied for the system of neighborhoods U_α, and also for the system of neighborhoods U'_α. It follows from this that the system of sets V_α satisfies the conditions of Theorem 10 with respect to the abstract group H. We shall take the system V_α for a complete system of neighborhoods of the identity of the topological group H (see Theorem 10).

We associate with every element $z = (x, x') \in K$ the element $x \in G$, $g(z) = x$. It is easy to see that g is a homomorphic mapping of the abstract group K on the abstract group G. It follows from this that g is also a homomorphic mapping of the group H on some subgroup G^* of the abstract group G. We shall show that $G^* = G$. In fact, $g(V) = U$, and hence $U \subset G^*$, but since G is generated by every neighborhood of the identity, it follows that $G \subset G^*$.

We shall now show that g is an open homomorphic mapping of the topological group H on the topological group G. It follows from the relation $g(V_\alpha) = U_\alpha$. that the mapping g is both continuous and open at the identity. Hence g is an open continuous mapping (see §19, B)).

By Theorem 12 the group G is isomorphic with the factor group H/N, where N is the kernel of the homomorphism g. We shall show that N is a discrete normal subgroup of the group H. To do this, it is sufficient to show that there exists a neighborhood of the identity of the group H which contains no element of the group N other than the identity. This condition is satisfied by any neighborhood of the system V_α, since the mapping g on the set V_α is one-to-one.

Similarly we can prove that G' is isomorphic with the factor group H/N', where N' is a discrete normal subgroup of the topological group H. This completes the proof of the theorem.

The statement of Theorem 18 will be further developed in Chapter VIII, however only for groups of a special type. We shall there find a corresponding group H for the whole class of groups locally isomorphic to a given group. Such a result enables us to divide the study of topological groups into the study of local properties and the study of the group as a whole.

By *local properties* of topological groups we shall understand those properties which hold for all locally isomorphic groups. It is worth noting that the local behavior of a group influences its behavior in the large to a great degree, and therefore the study of local properties is rather important.

Since in order to study local properties of a topological group G we need be interested only in the behavior of the group G in an arbitrarly small neighborhood U of the identity, the question naturally arises whether it is not possible to study the neighborhood U as an independent entity, without reference to the group G as a whole. This is the point of view of the classical theory of Lie groups (see Chapters VI and IX). We study there an entity which later turns out to be a neighborhood of the identity of an entire topological Lie group. I give here the exact definition of the corresponding logical concept. All that follows in this section is necessary only for the understanding of Chapters VI, VII, and IX.

D) A topological space G is called a *local group* if for some pairs a, b of elements of G a *product* $ab \in G$ is defined, and if the following conditions are satisfied:

a) If the products ab, $(ab)c$, bc, $a(bc)$ are defined, then $(ab)c = a(bc)$.

b) If the product ab is defined, there exist neighborhoods U' and V' of the elements a and b such that for $a' \in U'$ and $b' \in V'$, the product $a'b'$ is defined. Furthermore the law of multiplication for the pair a, b is continuous, i.e., for every neighborhood W of the product ab there exist neighborhoods U and V of the elements a and b for which $UV \subset W$.

c) G contains an element e which plays a special part and is called the *identity*. It possesses the following property: if $a \in G$, then the product ae is defined and $ae = a$.

d) If the product of the pair a, b is defined and $ab = e$, we say that b is a *right inverse* element of a, or $b = a^{-1}$. If a has a right inverse element a^{-1}, then there exists a neighborhood U' of the element a such that for every $a' \in U'$ there exists a right inverse element a'^{-1}. Furthermore, for every neighborhood V of the element a^{-1} there exists a neighborhood U of the element a such that $U^{-1} \subset V$.

E) If G is a local group and n an arbitrary integer there exists in G a sufficiently small neighborhood U of the identity e such that for every element $a \in U$ there exists an inverse a^{-1} in G, and for every set of n elements $a_1, \cdots, a_n$ of the neighborhood U, the product

$$(\cdots((a_1a_2)a_3)\cdots a_n) = b$$

is defined and does not depend on the distribution of the parentheses. We can therefore write $b = a_1 \cdots a_n$.

From condition c) it follows that the product ee is defined and that $ee = e$. From this and from conditions b) and c) follow the existence of a neighborhood W of the identity such that for any $a \in W$, there exists an inverse element a^{-1}, and for $a \in W$, $b \in W$, the product ab is defined. Furthermore, from the condition of continuity follows the existence of a neighborhood V such that $V^2 \subset W$. It is easy to see that condition E) is satisfied for V with $n = 3$. Continuing the construction further we shall obtain the desired neighborhood U for an arbitrary integer n.

F) If G is a local group, then there exist neighborhoods U and $V \subset U$ of the identity such that the following conditions are satisfied:

a) If $a \in U$, the product ea is defined and $ea = a$.

b) if $a \in U$, there exists an element a^{-1} such that the products aa^{-1} and $a^{-1}a$ are defined, and $aa^{-1} = a^{-1}a = e$.

c) If the elements a and b belong to V, then the equations $ax = b$ and $ya = b$ are solvable in the neighborhood U, and in that neighborhood each of these equations has a unique solution.

The assertion F) can be proved just as B) and C) were proved in §1, except that we have to select sufficiently small neighborhoods U and V in order that

all the operation which we have carried out in §1 should be possible. The existence of such small neighborhoods U and V is guaranteed by proposition E).

G) Let G be a local group. Every neighborhood U of the identity e of the group G we shall call a *part* of the local group G. Every part U of the local group G is itself a local group by virtue of the same operations which hold in G. In particular, we shall consider that the product ab is defined in U if it is defined in G and belongs to U.

H) Let G and G' be two local groups, and U, U' parts of G, G' respectively. We say that f is a *locally isomorphic* mapping of the group G on the group G' if f is a topological mapping of the part U on the part U', and if the following conditions are fulfilled. If the product ab is defined in U, then the product $f(a)f(b)$ is defined in U' and $f(ab) = f(a)f(b)$. The identity goes over into the identity under the mapping f. Finally the mapping f^{-1} must satisfy the same conditions that f satisfies. We say that two local groups G and G' are *locally isomorphic* if there exists a locally isomorphic mapping of one group on the other.

Two locally isomorphic mappings f and f' of the group G on the group G' are called *equivalent* if they coincide on some part of the group G. In what follows we shall study local isomorphisms only up to equivalence.

It is obvious that Definiton 30 is a special case of definition H) when the local groups G and G' are entire groups.

The true object of our investigation is not the local group itself, i.e., our concern is not with all of its properties, but only with those which remain invariant under locally isomorphic transformations. We are therefore interested in those constructions in local groups which remain invariant under locally isomorphic transformations.

Here a problem arises which is connected with the concept of a local group. Is every local group locally isomorphic with some topological group? This question is answered in the affirmative only for Lie groups, and even then by the application of a very complicated and special process (see §54).

We now go over to the definitions of other fundamental concepts, such as the subgroup, normal subgroup, factor group and homomorphic mapping for local groups.

I) Let G be a local group and H one of its subsets containing e. By Definition 16, H is a topological space. Furthermore we shall consider that the product ab of a pair of elements a, b of H is defined if it is defined in G and belongs to H. If the topological and algebraic operations thus defined in H satisfy the conditions of definition D), then H is itself a local group. If, moreover, there exists a neighborhood U of the identity of G in which the intersection $U \cap H$ is closed, then H is called a *subgroup* of the local group G. A local subgroup N of a local group G is called a *normal subgroup* if there exists a neighborhood V of the identity e in G such that for $x \in V$ and $y \in V \cap H$ we have $x^{-1}yx \in H$.

Two subgroups H and H' of the local group G are called *equivalent* if they have a common part (see G)), i.e., if they coincide in some neighborhood of the

identity. It can readily be seen that the class of all equivalent local subgroups of the group G is invariant under locally isomorphic transformations. It is such a class of subgroups that we shall be studying, i.e., we shall investigate the structure of a subgroup H only with reference to the properties common to all subgroups equivalent to H.

J) Let G be a local group, and N a normal subgroup. Let us construct the factor group $G^* = G/N$. To do this we select a neighborhood U of the identity in G, whose smallness will be determined by future constructions. We shall decompose the set U into cosets of the normal subgroup N, putting the elements x and y of U in the same class if $xy^{-1} \varepsilon N$. If U is sufficiently small all the axioms of equivalence (see §2, C)) will be satisfied. We can represent every coset X in the form $X = U \cap (Nx)$, where x is an arbitrary element of X. Conversely every set of the form $U \cap (Nx)$, where $x \varepsilon U$, will represent a coset. Furthermore, there exists a neighborhood V of the identity e in G sufficiently small so that if X and Y are cosets intersecting V, then $U \cap (XY) = Z$ is also a coset. If Z also intersects V, then we shall say that we have defined the product $XY = Z$. We denote by G^* the set of all cosets which intersect V. We introduce a topology into G^* in a natural way, as was done in Definition 24. By virtue of the established operations the set G^* becomes a local group and is called a *factor* group.

It is clear that the group $G/N = G^*$ is not uniquely defined when a group G and one of its normal subgroup N are given, but depends also on the choice of the neighborhoods U and V. It is not hard to see, however, that all the factor groups thus obtained are locally isomorphic with one another, so that those properties of the group G/N in which we are interested are uniquely determined. In the same way if we replace the normal subgroup N by an equivalent normal subgroup N', we obtain a factor group G/N' locally isomorphic with the factor group G/N.

K) Let G and G^* be two local groups, and U, U^* parts of G, G^* respectively. We say that f is a *locally homomorphic* mapping of the group G on the group G^* if f is an open continuous mapping of the part U on the part U^* satisfying the following conditions: If the product ab is defined in U, then the product $f(a)f(b)$ is defined in U^* and $f(ab) = f(a)f(b)$. Moreover, the identity goes over into the identity under the mapping f.

The set N of elements which go over into the identity under the mapping f is called the *kernel* of the homomorphism f, and is a normal subgroup of the local group G. It can also be shown that the group G^* is locally isomorphic with the factor group G/N.

Two locally homomorphic mappings f and f' of the group G on the group G^* are called *equivalent* if they coincide in some part of the group G. In what follows we shall study local homomorphism only up to equivalence.

L) We say that the local group G is *decomposed* into the *direct product* of normal subgroups H and K if there exist parts X, Y, Z of the local groups $H, K,$ and G such that every element $z \varepsilon Z$ is uniquely and continuously decom-

posed into the product xy, where $x \varepsilon X$, $y \varepsilon Y$. Continuity means that the elements x and y, uniquely determined from the equation $z = xy$, are continuous functions of the element z.

Obviously if the local groups H and K are given only up to a local isomorphism, the local group G is also defined only up to an isomorphism. This construction of the group G from the groups H and K can be carried out as in §15.

We have now transferred all the fundmaental concepts and relations of topological groups to local groups. We shall introduce here one more rather special, but nevertheless important concept.

M) Let G be a local group. We shall say that G has a *one parameter subgroup* $g(t)$, $|t| \leqq \alpha$, if in G an element $g(t)$ is given which depends continuously on a real parameter t and which is defined for all values of t not exceeding α in absolute value, and if the following conditions are satisfied: $g(0) = e$, and if $|s| \leqq \alpha$, $|t| \leqq \alpha$, and $|s + t| \leqq \alpha$, then the product $g(s)\,g(t)$ is defined and $g(s)g(t) = g(s + t)$. Obviously if G is a topological group, then the one parameter subgroup $g(t)$ can be extended to arbitrarily large values of α, making use of the relation $g(s)g(t) = g(s + t)$ as a defining operation.

EXAMPLE 35. Let G be the additive topological group of real numbers, and N the subgroup of all integers. By C) the groups G and G/N are locally isomorphic. It is obvious however that these groups are not isomorphic, since the first of them is not compact while the second one is. We have here the simplest example of locally isomorphic groups. More complicated examples will be given later.

EXAMPLE 36. Let G^n be the additive topological group of vectors in n-dimensional Euclidean space, given in cartesian coordinates. Let us denote by G^k the subgroup of G^n which is generated by the first k coordinate axes, and by N^k the totality of all the vectors in the space G^k having integral coordinates. N^k is a discrete subgroup of the group G^n and therefore the factor group $G^n/N^k = G^n_k$ is locally isomorphic with the group G^n (see C)). Hence all the groups G^n_k, $k = 0, 1, \cdots, n$, are locally isomorphic with one another, but no two of these groups are isomorphic or even homomorphic. The group G^n_n is compact, while all the other groups are not compact. The group G^n_0 is isomorphic with the group G^n.

It turns out that every connected group G which is locally isomorphic with the group G^n is isomorphic with one of the groups G^n_k.

CHAPTER IV

REPRESENTATIONS OF COMPACT TOPOLOGICAL GROUPS

In the preceding chapter the general theory of topological groups was developed. The concepts and relations considered there were of the most general type. The next problem consists of a deeper and constructive study of topological groups. It is desirable to connect general topological groups with more concrete subjects which can be studied independently with less difficulty. Such subjects are for example groups of matrices and Lie Groups (for the latter see Chapters 6 and 9). Such a connection would enable us to reduce questions about topological groups to corresponding questions about more elementary subjects. Moreover, we shall be able to construct topological groups of a very general type from particular topological groups. The method which we shall employ here is the method of representations.

We say that the topological group G admits a *representation* if there exists a homomorphism A of the group G into a topological group of matrices.

It is obvious, however, that every group admits a trivial representation in which all the elements of the group go into the identity of the group of matrices. Such a trivial representation can of course be of no help to us in the study of topological groups. The question therefore arises as to the existence of a non-trivial representation for a given group, or, what is even more, the question of the existence of a complete system of representations.

We say that a group G admits a *complete system of representations* if for each element g of the group G distinct from the identity there exists a representation of G under which g does not go over into the unit matrix.

The question of the existence of a complete system of representations for an arbitrary locally compact topological group satisfying the second axiom of countability has as yet not been solved. On its solution depends the solution of the central problems of the theory of topological groups. We can, however, construct the complete system of representations for every compact topological group satisfying the second axiom of countability. This chapter is devoted to the exposition of this construction. Some supplementary results will be given in Chapters V and VII.

The first step in the construction is to establish on the group an *invariant measure*, or what is the same, an *invariant integration*. Speaking more precisely, we assign to every set M of elements of G some non-negative number as its *measure* in such a way as to fulfill the condition of *invariance*, i.e., the measure of the set M is equal to the measure of the set Ma for any element a of the group G. If a group G has an invariant measure, then invariant integration can be established in it. Originally, an invariant measure in locally compact groups satisfying the second axiom of countability was constructed by Haar [11]. A little later von Neumann [22] independently constructed an invari-

ant integration in compact groups with the second axiom of countability. von Neumann's construction is considerably simpler, and since in the future we shall use invariant integration for compact groups only, we shall make use here of the work of von Neumann.

Before the construction of invariant integration was used for general compact topological groups, it was used by Peter and Weyl [24] for the construction of a complete system of representations for compact Lie groups, for which invariant integration is established rather simply. Peter and Weyl considered for their purposes some integral equations on a group, and in doing this they have essentially used the compactness of the group. As a result of the work of Haar their construction can be automatically applied to compact topological groups. But it has not been possible to extend it to locally compact groups.

24. Continuous Functions on a Topological Group

The set of elements of a topological group G forms a topological space, and therefore we can consider continuous functions defined on G (see Definition 20). The fact that G is a group, however, enables us to formulate the definition of continuity in a slightly different way, and what is more, to introduce the concept of uniformly continuous functions.

A) Let G be a topological group, and M a set of its elements. The real valued function $f(x)$ defined on the space M (see Definition 16) is *continuous* at a point a of M (see Definition 20) if and only if there exists for every positive number ϵ a neighborhood V of the identity such that if $x \varepsilon M$ and $xa^{-1} \varepsilon V$, then $|f(x) - f(a)| < \epsilon$.

We shall first show the sufficiency of the above condition. If $xa^{-1} \varepsilon V$, then, and only then, $x \varepsilon Va = U$. Hence $x \varepsilon U \cap M$ and $|f(x) - f(a)| < \epsilon$, and since $U \cap M$ is a neighborhood of the point a in the space M, the condition of Definition 20 is fulfilled. If the function $f(x)$ is continuous at the point a (see Definition 20), then there exists for every positive number ϵ a neighborhood U' of the point a in the space M such that $|f(x) - f(a)| < \epsilon$ for $x \varepsilon U'$. Furthermore there exists a neighborhood U of the point a in the space G such that $U' = U \cap M$ (see §10, C)). But $Ua^{-1} = V$ is a neighborhood of the identity in G, and if $xa^{-1} \varepsilon V$, and $x \varepsilon M$, then $x \varepsilon U'$ and, therefore, $|f(x) - f(a)| < \epsilon$. Hence the above condition is also necessary.

B) Let M be a subset of a topological group G, and $f(x)$ a real valued function defined on M. The function $f(x)$ is called *uniformly continuous* if for every positive number ϵ there exists a neighborhood V of the identity such that $|f(x) - f(y)| < \epsilon$ for $xy^{-1} \varepsilon V$, $x \varepsilon M$, and $y \varepsilon M$. Together with this definition, we give another analogous definition. A function $f(x)$ is called *uniformly continuous* if for every positive ϵ there exists a neighborhood V' of the identity in the space G such that $|f(x) - f(y)| < \epsilon$ for $x^{-1}y \varepsilon V'$. The above two definitions of uniform continuity are in general not equivalent, but in all the cases in which we are interested they are actually equivalent (see C)). Obviously, a uniformly continuous function is continuous.

In some cases uniform continuity follows from ordinary continuity.

C) Let G be a topological group satisfying the second axiom of countability, and M a compact subset of G. The continuous function $f(x)$ defined on M is automatically uniformly continuous in both senses (see B)).

Let ϵ be an arbitrary positive number. Since $f(x)$ is continuous, for every point $a \varepsilon M$ there exists a neighborhood V_a of the identity of the group G such that if $xa^{-1} \varepsilon V_a$, and $x \varepsilon M$, then $|f(x) - f(a)| < \frac{1}{2}\epsilon$. Let us denote by W_a a neighborhood of the identity such that $W_a^2 \subset V_a$. Obviously, the system of all open sets of the form $W_a a$, where a is an arbitrary element of M, covers the whole set M. By Theorem 7 we can select from this covering a finite covering. Therefore there exists a finite sequence $a_1, \cdots, a_n$ of elements of the set M such that the system of open sets $W_{a_i}a_i$, $i = 1, 2, \cdots, n$, covers M. We denote by V the intersection of all open sets of the system W_{a_i}. Then V is a neighborhood of the identity in G. We shall show that if $xy^{-1} \varepsilon V$, $x \varepsilon M$, $y \varepsilon M$, then $|f(x) - f(y)| < \epsilon$. This will prove the uniform continuity of $f(x)$. Since the system $W_{a_i}a_i$ covers M, there exists a number k such that $ya_k^{-1} \varepsilon W_{a_k}$, and therefore $|f(y) - f(a_k)| < \frac{1}{2}\epsilon$. Furthermore we have $xa_k^{-1} = xy^{-1}ya_k^{-1} \varepsilon VW_{a_k} \subset W_{a_k}^2 \subset V_{a_k}$ so that $|f(x) - f(a_k)| < \frac{1}{2}\epsilon$. Combining the two inequalities we get $|f(x) - f(y)| < \epsilon$.

Together with the concept of uniformly continuous functions, there exists the important concept of an equi-continuous family or set of functions.

D) Let M be a subset of a topological group G. A set Δ of functions defined on M is called *equi-continuous* if for every positive number ϵ there exists a neighborhood V of the group G such that for $xy^{-1} \varepsilon V$, $x \varepsilon M$, and $y \varepsilon M$, we have $|f(x) - f(y)| < \epsilon$ for all functions f of the set Δ. Obviously all functions of an equi-continuous family are themselves uniformly continuous.

We shall now recall the concept of a uniformly convergent sequence of functions.

E) We say that a sequence $f_n(x)$, $n = 1, 2, \cdots$, of functions defined on a topological space M *converges uniformly* to the function $f(x)$ defined on M, if for every positive number ϵ there exists an integer m such that $|f(x) - f_n(x)| < \epsilon$ for $n > m$, and an arbitrary $x \varepsilon M$.

Just as in classical analysis, we can prove Cauchy's necessary and sufficient condition for uniform convergence, which can be stated as follows:

F) A sequence $f_n(x)$, $n = 1, 2, \cdots$, of functions defined on a topological space M is uniformly convergent if for every positive ϵ there exists a sufficiently large number m such that for $p > m$, $q > m$, we have $|f_p(x) - f_q(x)| < \epsilon$ for every $x \varepsilon M$.

G) If a sequence of continuous functions converges uniformly, then its limit is a continuous function. This proposition can be proved just as in classical analysis.

We shall now prove the following important theorem.

Theorem 19. *Let G be a topological group, satisfying the second axiom of countability, and M a compact subset of G. We denote by Δ an equi-continuous*

family of functions defined on M (see D)) *which are uniformly bounded, i.e., there exist real numbers l and l' such that $l \leq f(x) \leq l'$ for every function $f(x)$ of the family Δ and arbitrary $x \varepsilon M$. Then a uniformly convergent subsequence can be selected from any sequence $\Delta' = \{f_1(x), \cdots, f_n(x), \cdots\}$ of functions of the family Δ* (see E)).

PROOF. Let us note first of all that M contains a countable everywhere dense set N (see §17, B)). For since G satisfies the second axiom of countability, M contains a countable basis. Taking one point from every open set of the basis, we get a countable set N everywhere dense in M. Let us number all the points of the set N by setting $N = \{a_1, \cdots, a_i, \cdots\}$, and let us consider the system $f_n(a_i)$, $n = 1, 2, \cdots, i = 1, 2, \cdots$, of real numbers. All these numbers lie on the interval between l and l', and therefore Theorem 9 is applicable here. Hence there exists an increasing sequence $n(1), n(2), \cdots, n(k), \cdots$ of integers such that the subsequence $f_{n(k)}(a_i)$, $k = 1, 2, \cdots$, converges for a fixed i. Letting $f_{n(k)}(x) = g_k(x)$, $k = 1, 2, \cdots$, we get a sequence $\Delta'' = \{g_1(x), \cdots, g_n(x), \cdots\}$ which converges at every point $a_i \varepsilon N$. We shall show that the sequence Δ'' converges uniformly on M.

Let ϵ be a positive number. Since the family Δ is equi-continuous there exists a neighborhood V of the identity of the group G such that if $xy^{-1} \varepsilon V$, $x \varepsilon M$, $y \varepsilon M$, then $|g_n(x) - g_n(y)| < \frac{1}{3}\epsilon$ for an arbitrary n. Since the set N is everywhere dense in M, the system of regions Va_k, $k = 1, 2, \cdots$, covers M. By Theorem 7 a finite covering can be selected from this covering, i.e., there exists a finite system of points $a_{k_j} = b_j$, $j = 1, \cdots, h$, such that the system of open sets Vb_j, $j = 1, \cdots, h$, covers G. Since the point b_j belongs to N, the sequence of numbers $g_n(b_j)$, $n = 1, 2, \cdots$, converges, and therefore there exists a sufficiently large number m_j such that $|g_p(b_j) - g_q(b_j)| < \frac{1}{3}\epsilon$ for $p > m_j$, and $q > m_j$. Denote by m' the maximum of the numbers m_j, $j = 1, \cdots, h$. Then $g_p(b_j) - g_q(b_j) < \frac{1}{3}\epsilon$ for $p > m'$, $q > m'$ and $j = 1, \cdots, h$. Let x be any point of M. Since the system of open sets Vb_j, $j = 1, \cdots, h$ covers M there exists a point b_i such that $xb_i^{-1} \varepsilon V$ and hence $|g_p(x) - g_p(b_i)| < \frac{1}{3}\epsilon$, and $|g_q(x) - g_q(b_i)| < \frac{1}{3}\epsilon$. Combining the last inequalities we get $|g_p(x) - g_q(x)| < \epsilon$. Hence the criterion F) of uniform convergence is satisfied for the sequence Δ'' and therefore this sequence is uniformly convergent.

We shall make one more remark concerning continuous functions.

H) Let M be a compact topological space and $f(x)$ a continuous function defined on M (see Definition 20). We denote the minimum of the function $f(x)$ by $K(f(x))$ and the maximum by $L(f(x))$ (see §14, B)). The number $S(f(x)) = L(f(x)) - K(f(x))$ is called the *variation* of the function $f(x)$. If the sequence $f_n(x)$, $n = 1, 2, \cdots$, of continuous functions converges uniformly to the function $f(x)$ (see E)), then the following relations hold, as may be easily verified:

$$\lim_{n\to\infty} K(f_n(x)) = K(f(x)), \quad \lim_{n\to\infty} L(f_n(x)) = L(f(x)), \quad \lim_{n\to\infty} S(f_n(x)) = S(f(x)).$$

Example 37. Let G be a compact topological group satisfying the second axiom of countability. Let us consider the set R of all continuous functions on G. We can introduce a distance into the set R in a natural way by defining the distance between two continuous functions $f(x)$ and $g(x)$ defined on G, i.e., between two elements of R, as the maximum of $|f(x) - g(x)|$. It is easy to show that R is a metric space (see Example 14). In the first place the maximum of $|f(x) - g(x)|$ is equal to zero if and only if $f(x) = g(x)$. Furthermore if $f(x)$, $g(x)$, and $h(x)$ are three continuous functions defined on G then $|f(x) - h(x)| \leqq |f(x) - g(x)| + |g(x) - h(x)|$, from which the triangle axiom in R follows.

It is easy to formulate the condition of uniform convergence of a sequence of functions $f_n(x)$, $n = 1, 2, \cdots$, to a function $f(x)$ in terms of the metric space R. This convergence exists if and only if the sequence $f_n(x)$, $n = 1, 2, \cdots$, converges to $f(x)$ in the sense of a metric defined in the space R.

Let Δ be a uniformly bounded equi-continuous family of functions defined on G. Then $\Delta \subset R$. It follows from Theorem 19 that the closure $\bar{\Delta}$ of the set Δ in the space R is compact.

Example 38. Let G be the additive topological group of real numbers, and M a closed interval on the real axis. The propositions given in this section then become the well known propositions of classical analysis.

25. Invariant Integration

This section is devoted to the exposition of the work of von Neumann in which he gives the construction of invariant integration in a compact topological group satisfying the second axiom of countability.

Definition 31. We say that an *invariant integration* is defined over a compact topological group G if the following conditions are satisfied.

1) To every real continuous function $f(x)$ defined on G (see Definition 20) corresponds a real number, which we designate symbolically by $\int f(x)dx$, and call the *integral* of the function $f(x)$ over the group G.

2) If α is a real number, then $\int \alpha f(x)dx = \alpha \int f(x)dx$, i.e., in integration a constant multiplier can be taken outside the integral sign.

3) If $f(x)$ and $g(x)$ are two continuous functions, then

$$\int (f(x) + g(x))dx = \int f(x)dx + \int g(x)dx.$$

4) If $f(x)$ is always non-negative, then $\int f(x)dx \geqq 0$.

5) If $f(x) = 1$ for every x, then $\int f(x)dx = 1$.

6) If the function $f(x)$ is non-negative and is not identically zero, then $\int f(x)dx > 0$.

7) If a is an element of G, then

$$\int f(xa)dx = \int f(x)dx.$$

8) If a is an element of G, then

$$\int f(ax)dx = \int f(x)dx.$$

9)
$$\int f(x^{-1})dx = \int f(x)dx.$$

The first six conditions are natural for any concept of integration, while the last three express special properties of group invariance.

We note that conditions 2), 3), and 4) make possible the integration of inequalities and absolute values; in fact, if $f(x) \leqq g(x)$, then

$$\int f(x)dx \leqq \int g(x)dx, \qquad \left|\int f(x)dx\right| \leqq \int |f(x)|\,dx.$$

For if $g(x) - f(x) \geqq 0$, it follows from 4) that $\int(g(x) - f(x))dx \geqq 0$, and by 2) and 3) this relation can be written in the form

$$\int g(x)dx - \int f(x)dx \geqq 0, \quad \text{i.e.,} \quad \int f(x)dx \leqq \int g(x)dx.$$

Furthermore $-|f(x)| \leqq f(x) \leqq |f(x)|$ and by the integration of inequalities just established we have $-\int|f(x)|dx \leqq \int f(x)dx \leqq \int|f(x)|dx$ which can be written

$$\left|\int f(x)dx\right| \leqq \int |f(x)|\,dx$$

THEOREM 20. *It is possible to define uniquely invariant integration* (see Definition 31) *over every compact topological group G satisfying the second axiom of countability. If an integral is defined which satisfies conditions* 1) *to* 5) *and* 7), *then the remaining conditions* 6), 8), *and* 9) *are also satisfied.*

The proof of Theorem 20 is not simple and is divided into a series of steps. We shall give these steps in the form of preliminary remarks, and shall denote only the concluding part as the proof of the theorem.

In what follows we shall understand by G a compact topological group satisfying the second axiom of countability.

A) Let G be a topological group, $f(x)$ a continuous function defined on G, and $A = \{a_1, \cdots, a_m\}$ a finite system of elements of the group G. We shall introduce the following notation:

(1)
$$M(A, f(x)) = \sum_{i=1}^{m} \frac{f(xa_i)}{m}.$$

The function $M(A, f(x))$ is continuous, and is fundamental in the construction of invariant integration. For it, as can easily be verified, the following relations hold (for notation see §24, H)):

(2) $$K(M(A, f(x))) \geqq K(f(x)),$$

(3) $$L(M(A, f(x))) \leqq L(f(x)),$$

(4) $$S(M(A, f(x))) \leqq S(f(x)).$$

Furthermore, if A and B are two finite systems of elements of G, then

(5) $$M(A, M(B, f(x))) = M(AB, f(x)).$$

B) If $f(x)$ is a non-constant continuous function defined on G, then there exists in G a finite system A of elements such that

(6) $$S(M(A, f(x))) < S(f(x))$$

(see A)).

Let k be the minimum and l the maximum of the function $f(x)$. Since $f(x)$ is continuous and $k < l$, there exists an open set $U \subset G$ such that for every $x \in U$ the inequality $f(x) \leqq h < l$ holds. The set of all open sets of the form Ua^{-1} covers the group G, and, therefore by Theorem 7 there exists a finite system $A = \{a_1, \cdots, a_m\}$ of elements of G such that the system of open sets Ua_i^{-1}, $i = 1, \cdots, m$, covers G. We shall show that the function $M(A, f(x))$ has a maximum which does not exceed $\dfrac{(m-1)l + h}{m} < l$. In fact for every x, $f(xa_i) \leqq l$, $i = 1, 2, \cdots, m$, but for any x a number j can be found such that $x \in Ua_j^{-1}$, i.e., $xa_j \in U$, and therefore $f(xa_j) \leqq h$. Since the minimum of the function $M(A, f(x))$ is not less than k (see (2)), the relation (6) is established.

C) Let $f(x)$ be a continuous function defined on the group G. We shall call a *right mean* of the function $f(x)$ any real number p which possesses the following property: For every positive ϵ there exists a finite system A of elements of the group G such that

(7) $$| M(A, f(x)) - p | < \epsilon.$$

We shall show that a continuous function $f(x)$ defined on G has at least one right mean.

Let us denote by Δ the totality of all functions of the type $M(A, f(x))$, where $f(x)$ is a given function, and A is an arbitrary finite system of elements of G. It follows from 2) and 3) that the family Δ is uniformly bounded. We shall show that it is equi-continuous (see §24, D)).

Being continuous, the function $f(x)$ is uniformly continuous (see §24, C)). Therefore for every positive ϵ a neighborhood V of the identity can be found such that $|f(x) - f(y)| < \epsilon$ for $xy^{-1} \in V$. But since $xy^{-1} \in V$, it is also true that $(xa_i)(ya_i)^{-1} = xy^{-1} \in V$. Hence $|f(xa_i) - f(ya_i)| < \epsilon$. Summing this inequality over i from 1 to m and dividing the result by m, we obtain $|M(A, f(x)) - M(A, f(y))| < \epsilon$. The last inequality holds for $xy^{-1} \in V$, and for an arbitrary system A. Hence the family Δ is equi-continuous.

We denote by s the lower bound of all the numbers $S(M(A, f(x)))$, i.e., the lower bound of the variations of all the functions belonging to Δ. Then there exists a sequence

$$(8) \qquad f_1(x), \cdots, f_n(x), \cdots$$

of functions of Δ such that

$$\lim_{n\to\infty} S(f_n(x)) = s.$$

Since the family Δ is uniformly bounded and equi-continuous, it follows from Theorem 19 that we can select from the sequence (8) a uniformly convergent subsequence

$$(9) \qquad g_1(x), \cdots, g_n(x), \cdots$$

whose limit we denote by $g(x)$. We have $S(g(x)) = s$ (see §24, H)). We shall show that the function $g(x)$ is a constant or, what is the same, that $s = 0$.

Let us suppose that $g(x)$ is not a constant. Then it follows from B) that there exists a finite system A of elements of G such that

$$(10) \qquad S(M(A, g(x))) = s' < s.$$

Let $\epsilon = \frac{1}{3}(s - s')$. Since the sequence (9) converges uniformly to $g(x)$, there exists a number k for which $|g(x) - g_k(x)| < \epsilon$. Replacing x in the last inequality by xa_i and summing all the inequalities thus obtained over i from 1 to m and dividing by m, we obtain

$$(11) \qquad | M(A, g(x)) - M(A, g_k(x)) | < \epsilon.$$

It follows from inequalities 10) and 11) that

$$S(M(A, g_k(x))) \leqq s' + 2\epsilon < s.$$

But by (5) the function $M(A, g_k(x))$ belongs to Δ so that we have arrived at a contradiction, since the lower bound of the variations of all the functions belonging to Δ is equal to s by assumption. Hence the function $g(x)$ is a constant: $g(x) = p$.

Since the sequence 9) converges uniformly to $g(x) = p$, there exists for every positive ϵ a number n such that $|g_n(x) - p| < \epsilon$. But $g_n(x) \in \Delta$, and therefore for every positive ϵ there exists a system A of elements of G for which the inequality 7) holds.

D) By analogy with A) we introduce a new function by letting

$$(12) \qquad M'(B, f(x)) = \sum_{j=1}^{n} \frac{f(b_j x)}{n}$$

where $B = \{b_1, \cdots, b_n\}$. It can be readily verified that

$$(13) \qquad M(A, M'(B, f(x))) = M'(B, M(A, f(x))).$$

E) By analogy with C) we introduce the left mean. We shall call a real number q a *left mean* of a continuous function $f(x)$ defined on G, if it possesses the following property: For every positive number ϵ there exists a finite system B of elements of the group G such that

$$(14) \qquad | M'(B, f(x)) - q | < \epsilon.$$

We shall show that there exists at least one left mean for every continuous function defined on G. To do this we retain the topology of G, but introduce into G the operation of multiplication in a different way. The new topological group thus obtained we shall denote by G'. We shall define the product $a \times b$ in the group G' by suppose that $a \times b = ba$, where ba is the product in the group G. It is not hard to verify that this method gives rise to a topological group G'. It is also not hard to see that a right mean of the group G' is a left mean of the group G, but as the existence of a right mean has already been established, we arrive at the existence of a left mean.

F) For every continuous function $f(x)$ defined on G there exists only one right mean and one left mean and these means coincide. The unique mean thus obtained is called the *mean* of the function $f(x)$ and is denoted by $M(f(x))$.

Let p be some right mean of the function $f(x)$, and q some left mean of the same function. Then relations (7) and (14) hold. Putting into (7) the element $b_j x$ instead of x and summing over j from 1 to n and dividing the result by n we get

$$(15) \qquad | M'(B, M(A, f(x))) - p | < \epsilon.$$

Substituting xa_i instead of x in (14) and summing over i from 1 to m, we get after dividing by m,

$$(16) \qquad | M(A, M'(B, f(x))) - q | < \epsilon.$$

From the inequalities (15), (16), and relation (13) we obtain $|p - q| < 2\epsilon$. Since the last inequality holds for an arbitrary positive ϵ, it follows that $p = q$. Hence every right mean is equal to every left mean and proposition F) is proved.

G) If $f(x)$ and $g(x)$ are two continuous functions defined on the group G, then

$$(17) \qquad M(f(x) + g(x)) = M(f(x)) + M(g(x))$$

(see F)). We shall show first that

$$(18) \qquad M(M(B, f(x))) = M(f(x)).$$

Let

$$(19) \qquad M(f(x)) = p$$

Then p is a left mean of $f(x)$, and there exists for a positive ϵ a system C of elements of the group G such that

$$| M'(C, f(x)) - p | < \epsilon$$

Replacing x in the last relation by xb_j and summing over j from 1 to n, we obtain after division by n,

$$| M(B, M'(C, f(x))) - p | < \epsilon.$$

This last inequality may be written in the form

$$| M'(C, M(B, f(x))) - p | < \epsilon$$

by making use of (13). Hence p is a left mean of $M(B, f(x))$ and, therefore, relation (18) is fulfilled.

Let

$$M(g(x)) = q. \tag{20}$$

Then q is the right mean for $g(x)$ and hence there exists for an arbitrary positive ϵ a finite system B of elements of the group G such that

$$| M(B, g(x)) - q | < \epsilon.$$

From this inequality it follows that

$$| M(A', M(B, g(x))) - q | < \epsilon,$$

where A' is an arbitrary finite system of elements. From (5) we have

$$| M(A'B, g(x)) - q | < \epsilon. \tag{21}$$

From (18) and (19), it follows that p is a right mean of $M(B, f(x))$, i.e., there exists a finite system A of elements of the group G such that

$$| M(A, M(B, f(x))) - p | < \epsilon$$

and this can be written in view of (5) in the form

$$| M(AB, f(x)) - p | < \epsilon. \tag{22}$$

Relations (21) and (22) give for $A = A'$,

$$| M(AB, f(x) + g(x)) - (p + q) | < 2\epsilon.$$

Therefore, $p + q$ is a right mean for the sum $f(x) + g(x)$, which proves (17).

H) Let $f(x)$ be a continuous function defined on G, and a an arbitrary element of the group G. Then

$$M(f(xac) = M(f(x)), \tag{23}$$

$$M(f(ax)) = M(f(x)). \tag{24}$$

We remark first of all that

$$M(A, f(xa)) = M(Aa, f(x))$$

(see (1)). It follows from this relation that the right means of the functions $f(xa)$ and $f(x)$ co'ncide, from which it follows that equation (23) is satisfied.

Relation (24) can be established in an analogous way by making use of the left mean.

I) If $f(x)$ is a non-negative continuous function defined on G which is not identically zero, then

$$M(f(x)) > 0. \tag{25}$$

It can readily be seen that there exists an open set $U \subset G$ such that $f(x) > h > 0$ for $x \varepsilon U$. The set of all open sets of the form Ua^{-1} covers G and by Theorem 7 we can select from this covering a finite covering, i.e., there exists a system of elements $A = \{a_1, \cdots, a_m\}$ such that the system of open sets Ua_i^{-1}, $i = 1, \cdots, m$, covers G. For every x we have $f(x) \geqq 0$, and also for any x a number k can be found such that $x \varepsilon Ua_k^{-1}$, i.e. $xa_k \varepsilon U$, and hence $f(xa_k) > h$. In this way $M(A, f(x)) \geqq h/m$, i.e. $M(f(x)) = M(M(A, f(x))) \geqq h/m$ (see (1) and (18)).

Proof of Theorem 20. We define the integral $\int f(x)dx$ of any continuous function defined on G by setting

$$\int f(x)dx = M(f(x)) \tag{26}$$

(see F)). In this way condition 1) of Definition 31 is satisfied.

The fact that conditions 2), 4), and 5) of Definition 31 hold is established rather simply, while the fulfillment of conditions 3), 6), 7), and 8) follows from propositions G), I), and H) established above.

We shall now show that if we define an integral $\int^* f(x)dx$ in such a way that it satisfies conditions 1) to 5) and 7) of Definition 31, then

$$\int^* f(x)dx = M(f(x)). \tag{27}$$

Let p be a right mean of the function $f(x)$. Then we have

$$|M(A, f(x)) - p| < \epsilon.$$

This inequality can be integrated because conditions 2), 3), and 4) of Definition 31 hold. We obtain by making use of 2), 5), and 7),

$$\left|\int^* M(A, f(x))dx - p\right| = \left|\int^* f(x)dx - p\right| \leqq \epsilon. \tag{28}$$

Since inequality (28) holds for any positive ϵ, relation (27) follows at once.

Hence the uniqueness of the integral satisfying condition 1) to 5) and 7) of Definition 31 is established.

It remains to be proved that condition 9) of Definition 31 is fulfilled. To do this we define on G the integral $\int^* f(x)dx$ by setting

$$\int^* f(x)dx = M(f(x^{-1})). \tag{29}$$

It is not hard to check that conditions 1) to 5) and 7) of Definition 31 hold for this integral. We shall go through the verification of condition 7) only. We have

$$\int^* f(xa)dx = M(f(x^{-1}a)) = M(f((a^{-1}x)^{-1})) = M(f(x^{-1})) = \int^* f(x)dx$$

(see (24)). Because of the uniqueness established above we have $M(f(x^{-1})) = M(f(x))$, which completes the proof of Theorem 20.

In what follows we shall use integration not only with respect to one variable, but also with respect to two variables. It is therefore necessary to prove that the result of integration does not depend on the order of integration.

J) Let G and H be two compact topological groups satisfying the second axiom of countability, and $f(x, y)$ a continuous function of two variables $x \varepsilon G$ and $y \varepsilon H$ (see §15, G)). For a fixed y, the function $f(x, y)$ is a continuous function of x. We can therefore form the integral $\int f(x, y)dx = g(y)$ (see Definition 31 and Theorem 20). Then $g(y)$ is a continuous function defined on the group H.

Let P be the direct product of the topological groups G and H (see Definition 28′). Then the function $f(x, y)$ can be treated as a continuous function $f(z)$ of a single variable $z = (x, y) \varepsilon P$, defined on P (see §15, G)). Since the group P is compact and satisfies the second axiom of countability (see §15, E) and C)), the function $f(z)$, being continuous, is also uniformly continuous (see §24, C)). Hence for a given positive ϵ there exists a neighborhood W of the identity of the group P such that $|f(z') - f(z)| < \epsilon$ for $z'z^{-1} \varepsilon W$. The neighborhood W is composed of all pairs (x, y) such that $x \varepsilon U$, $y \varepsilon V$, where U and V are neighborhoods of the identities of the groups G and H (see Definition 21). Hence if $x'x^{-1} \varepsilon U$, $y'y^{-1} \varepsilon V$, then $|f(x', y') - f(x, y)| < \epsilon$. In particular for $y'y^{-1} \varepsilon V$, we have $|f(x, y') - f(x, y)| < \epsilon$, from which it follows that

$$| g(y') - g(y) | \leq \int | f(x, y') - f(x, y) | \, dx < \epsilon,$$

i.e., $g(y)$ is a uniformly continuous function.

THEOREM 21. *Let G and H be two compact topological groups satisfying the second axiom of countability and $f(x, y)$ a continuous function of two variables $x \varepsilon G$, and $y \varepsilon H$* (see §15, G)). *Then we have the following relations*

$$\int \left(\int f(x, y)dx \right) dy = \int \left(\int f(x, y)dy \right) dx = \int\int f(x, y)dxdy.$$

(See Definition 31 and Theorem 20. The second integration in the first and second parts of this relation is permissible because the function under the integral sign is continuous (see J)). The last equality is a definition.

PROOF. Let P be the direct product of the groups G and H (see Definition 28′). P is compact and satisfies the second axiom of countability (see §15, E)

and C)). The function $f(x, y)$ can be considered as a continuous function $f(z)$ of a single variable $z = (x, y) \varepsilon P, f(z) = f(x, y)$ (see §15, G)). For a fixed y, $f(x, y)$ is a continuous function on G, and we can define $\int f(x, y)dx$. This integral taken as a function of y is continuous in H (see J)) and therefore we can define $\int(\int f(x, y)dx)dy$. We shall show that the integral thus obtained coincides with $\int f(z)dz$. To do this let $\int^* f(z)dz = \int(\int f(x, y)dx)dy$. It is not hard to see that the integral $\int^* f(z)dz$ satisfies all the conditions of Definition 31. Let us verify only condition 7). Let $c \varepsilon P$, where $c = (a, b)$ and $a \varepsilon G, b \varepsilon H$; then

$$\int^* f(zc)dz = \int\left(\int f(xa, yb)dx\right)dy = \int\left(\int f(x, yb)dx\right)dy$$
$$= \int\left(\int f(x, y)dx\right)dy = \int^* f(z)dz.$$

Hence, since invariant integration is unique (see Theorem 20),

$$\int\left(\int f(x, y)dx\right)dy = \int f(z)dz.$$

Similarly, it can also be shown that $\int(\int f(x, y)dy)dx = \int f(z)dz$, so that a double integral does not depend on the order of integration, and Theorem 21 is proved.

If the group H coincides with the group G then the function $f(x, y)$ is a continuous function of two variables defined on G. This gives the most important case.

Example 39. If the group G is finite, then the integral of a function over G is defined simply as the arithmetic mean of the values of this function on the elements of the group.

Example 40. Let G^* be the additive topological group of real numbers and $\varphi(x^*)$ a continuous periodic function of period one, defined on G^*, $\varphi(x^* + 1) = \varphi(x^*)$. We denote by N the subgroup of the group G^* composed of all integers. The function $\varphi(x^*)$, being periodic, assumes equal values on all elements of every coset of N in G^*. Hence to the function $\varphi(x^*)$ defined on G^* corresponds a continuous function $f(x)$ defined on the factor group $G^*/N = G$. And conversely, every continuous function $f(x)$ on G can be obtained in this way. Since the group G is compact, there exists on it an integral $\int f(x)dx$, satisfying the conditions of Definition 31. It is not hard to see that $\int f(x)dx = \int_0^1 \varphi(x^*)dx^*$, where on the right we have the ordinary integral of a function of a real variable.

26. Systems of Functions and Integral Equations on a Group

Making use of integration over a group (see the preceding section) it is possible to establish on a group a series of concepts and relations of ordinary analysis. To this we devote the present section.

In what follows we shall denote by G a compact topological group satisfying the second axiom of countability. *All the functions considered on G will be suppose to be continuous.* We shall assume here that the functions under consideration take on complex as well as real values. We shall denote by $\bar{x}$ the conjugate of x.

A) Two functions $\varphi(x)$ and $\psi(x)$ defined on G are called *orthogonal* if

$$\int \varphi(x)\bar{\psi}(x)dx = 0. \tag{1}$$

It is easy to see that relation (1) implies

$$\int \bar{\varphi}(x)\psi(x)dx = 0.$$

Hence the orthogonality relation is symmetric. A set Δ of functions defined on G is called an *orthogonal system* if any two distinct functions belonging to Δ are orthogonal. The orthogonal system Δ is called *orthonormal* if for every function $\varphi(x) \varepsilon \Delta$ we have

$$\int \varphi(x)\bar{\varphi}(x)dx = 1. \tag{2}$$

B) Let

$$\Delta = \{\varphi_1(x), \cdots, \varphi_i(x), \cdots\} \tag{3}$$

be a finite or countable orthonormal system of functions defined on G. Let $g(x)$ be a function defined on G, and let

$$h_i = \int g(x)\bar{\varphi}_i(x)dx. \tag{4}$$

The numbers h_i, $i = 1, 2, \cdots$, are called the Fourier coefficients of the function $g(x)$ with respect to the system (3). They satisfy the inequality

$$\sum_{i=1}^{\infty} h_i\bar{h}_i \leqq \int g(x)\bar{g}(x)dx. \tag{5}$$

To prove (5) we form the finite sum $g_n(x) = \sum_{i=1}^{n} h_i\varphi_i(x)$ and consider the integral

$$\int (g(x) - g_n(x))(\bar{g}(x) - \bar{g}_n(x))dx = \alpha.$$

Since we have under the integral sign the product of two complex conjugates and therefore a real non-negative quantity, it follows that $\alpha \geqq 0$. A simple calculation shows that

(6)
$$\alpha = \int g(x)\bar{g}(x)dx - \sum_{i=1}^{n} h_i\bar{h}_i.$$

But since $\alpha \geqq 0$, (5) follows from (6).

C) The orthonormal system (3) is called *complete* if for every function $g(x)$ we have instead of the inequality (5) the equality

(7)
$$\sum_{i=1}^{\infty} h_i\bar{h}_i = \int g(x)\bar{g}(x)dx.$$

If the orthogonal system Δ under consideration is not normal, it can be normalized by setting $\varphi_i^*(x) = \varphi_i(x)/\beta_i$, where $\beta_i = +\sqrt{[\int \varphi_i(x)\bar{\varphi}_i(x)dx]}$. The new orthogonal system $\varphi_i^*(x)$, $i = 1, 2, \cdots$, thus obtained is normal, and if it is complete the system Δ is also called complete.

D) A set Ω of functions given on G is called a *uniformly complete system* if for every function $g(x)$ defined on G and every positive ϵ, there exists a finite linear form $g^*(x) = \sum_{i=1}^{n} a_i\varphi_i(x)$, with constant coefficients a_i, $i = 1, 2, \cdots, n$, $\varphi_i(x) \in \Omega$, $i = 1, \cdots, n$, such that $|g(x) - g^*(x)| < \epsilon$.

E) Let

$$\Delta = \{\varphi_1(x), \cdots, \varphi_i(x), \cdots\}$$

be an orthogonal system of functions defined on G. If the system Δ is uniformly complete (see D)), then it is a complete orthogonal system of functions (see C)).

We shall assume for simplicity that the system Δ is normalized.

Let $g(x)$ be a function on G. We denote the Fourier coefficients of this function with respect to the system by h_i, $i = 1, 2, \cdots$. Let n be a fixed integer and $a_1, \cdots, a_n$ arbitrary numbers. Let us suppose that

$$g^*(x) = \sum_{i=1}^{n} a_i\varphi_i(x).$$

We shall now ask for what values of the numbers $a_1, \cdots, a_n$ the expression

$$\gamma = \int (g(x) - g^*(x))(\bar{g}(x) - \bar{g}^*(x))dx$$

achieves a minimum.

A straightforward calculation gives

$$\gamma = \int g(x)\bar{g}(x)dx - \sum_{i=1}^{n} (h_i\bar{a}_i + \bar{h}_i a_i) + \sum_{i=1}^{n} a_i\bar{a}_i.$$

Making a simple algebraic transformation we get

$$\gamma = \int g(x)\bar{g}(x)dx - \sum_{i=1}^{n} h_i\bar{h}_i + \sum_{i=1}^{n} (h_i - a_i)(\bar{h}_i - \bar{a}_i).$$

This formula shows that γ attains its minimum for $a_i = h_i$, $i = 1, \cdots, n$, and also that this minimum value is

$$\gamma' = \int g(x)\bar{g}(x)dx - \sum_{i=1}^{n} h_i\bar{h}_i.$$

We note now that since the system Δ is uniformly complete, we can select for every positive number ϵ an integer n and a set of numbers $a_1, \cdots, a_n$ such that $|g(x) - g^*(x)| < \epsilon$, and this shows that $\gamma < \epsilon^2$ for the indicated choice, and therefore the minimum value γ' of γ also does not exceed ϵ^2, i.e., we have

$$\int g(x)\bar{g}(x)dx - \sum_{i=1}^{n} h_i\bar{h}_i < \epsilon^2.$$

It follows from the last inequality combined with (5), that equation (7) is true.

F) If

$$\Delta = \{\varphi_1(x), \cdots, \varphi_i(x), \cdots\}$$

is a system of orthogonal functions defined on G which does not contain the identically zero function, then all its functions are linearly independent.

Let us suppose that there exists a linear relation $\sum_{i=1}^{n} b_i\varphi_i(x) = 0$. Multiplying this equation by $\bar{\varphi}_k(x)$ and integrating we obtain $b_k\int\varphi_k(x)\bar{\varphi}_k(x)dx = 0$. But since the function under the integral sign is non-negative and is not identically zero, the integral is positive and therefore $b_k = 0$ for every k.

THEOREM 22. *Let Δ be an orthogonal system of functions defined on the compact topological group G satisfying the second axiom of countability. Then the set Δ is at most countable.*

PROOF. Let us exclude from the system Δ the identically zero function, and let us normalize all the remaining functions. We denote the orthonormal system thus obtained by Ω and prove that Ω is at most a countable set.

Let Σ be a countable basis of the topological space G. We shall call a pair of open sets (U, V) of Σ *distinguished* if $\bar{V} \subset U$. The set of all distinguished pairs is countable, and therefore they can be numbered. Let (U_n, V_n), $n = 1, 2, \cdots$, be the set of all distinguished pairs. By Urysohn's Lemma (see §14) there exists on G a continuous function $g_n(x)$ which possesses the following properties: $0 \leqq g_n(x) \leqq 1$, $g_n(x) = 0$ for $x \in G - U_n$, $g_n(x) = 1$ for $x \in \bar{V}_n$.

We shall show that for every function $\varphi(x) \in \Omega$ there exists a number m such that $\int g_m(x)\bar{\varphi}(x)dx \neq 0$. In fact since $\varphi(x)$ is continuous and not identically zero, there exists a region W on which the real or imaginary part of the function $\varphi(x)$ does not change sign. Let m be a number such that $U_m \subset W$. It can readily be seen that $\int g_m(x)\bar{\varphi}(x)dx \neq 0$ (see Definition 31, 6)).

Let us now denote by $\Omega_n^{(k)}$ the set of all functions $\psi(x)$ of the system Ω for which

$$\left|\int g_n(x)\bar{\psi}(x)dx\right| > 1/k,$$

where k is an integer. Since the inequality (5) is applicable to each finite subsystem of the system $\Omega_n^{(k)}$, the number of functions of the system $\Omega_n^{(k)}$ does not exceed $k^2\int g_n(x)\bar{g}_n(x)dx$. Hence the set $\Omega_n^{(k)}$ is finite. On the other hand it has been shown above that for every function $\psi(x) \varepsilon \Omega$ there exists a number m such that $\int g_m(x)\bar{\varphi}(x)dx \neq 0$ and hence there exists a sufficiently large number k for which $\varphi(x) \varepsilon \Omega_m^{(k)}$.

Hence Ω is a countable sum of finite sets $\Omega_n^{(k)}$, $k = 1, 2, \cdots, n = 1, 2, \cdots$, and Theorem 22 is proved.

In the theory of representations of compact topological groups an important part is played by a certain integral equation on a group. We therefore stop here to review some results in the theory of integral equations which will be of use later.

G) Let $k(x, y)$ be a real continuous function of two variables defined on G (see §15, G)), which is *symmetric*, i.e.,

$$k(x, y) = k(y, x). \tag{8}$$

Let us consider the integral equation

$$\varphi(x) = \lambda \int k(x, y)\varphi(y)dy \tag{9}$$

where λ is a real parameter, and $\varphi(x)$ is a continuous real function. The values of the parameter λ for which there exists not identically zero solutions of equation (9) are called *characteristic values* of this equation, while the corresponding solutions are the *characteristic functions* belonging to a given characteristic value.

H) Let λ' be a characteristic value of equation (9) and Δ the totality of all characteristic functions belonging to this characteristic value. Then Δ is a *linear* system of functions, i.e., if $\varphi(x)$ and $\psi(x)$ are two functions of Δ, then Δ contains the functions $a\varphi(x) + b\psi(x)$, where a and b are arbitrary real numbers. Furthermore, Δ contains a finite orthogonal basis, i.e., it contains a finite orthonormal system of functions

$$\varphi_1(x), \cdots, \varphi_n(x), \cdots \tag{10}$$

such that all the other functions of Δ can be expressed as a linear combination of functions of (10).

The fact that the system Δ is linear can be checked easily. We shall show that the number of linearly independent functions of the system cannot exceed a certain fixed integer depending on the kernel $k(x, y)$ and the characteristic value λ'. Let

$$\varphi_i(x), \qquad i = 1, \cdots, m, \tag{11}$$

be a system of linearly independent functions of Δ. Without loss of generality we may suppose that the system (11) is orthonormal, for if it were not, it could

be replaced by such a system by means of a linear transformation without changing the number of its functions. Let

$$k^*(x, y) = \sum_{i=1}^{m} \frac{1}{\lambda'} \psi_i(x)\psi_i(y)$$

and let us consider

$$\delta = \iint (k(x, y) - k^*(x, y))^2 dxdy$$

(see Theorem 21). We have $\delta \geqq 0$. A straightforward calculation shows that

$$\delta = \iint (k(x, y))^2 dxdy - \frac{m}{\lambda'^2},$$

from which it follows that

$$m \leqq \lambda'^2 \iint (k(x, y))^2 dxdy.$$

Hence Δ contains a finite maximal system of linearly independent functions from which, by means of linear transformations, can be obtained an orthonormal system satisfying condition H).

We give without proof the following important fact in the theory of integral equations.

I) Let

$$g(x) = \int k(x, y)f(y)dy.$$

Then the function $g(x)$ can be represented as the sum of a uniformly convergent series of functions

$$g(x) = \varphi_1(x) + \cdots + \varphi_n(x) + \cdots$$

where $\varphi_n(x)$, $n = 1, 2, \cdots$, are characteristic functions of equation (9).*

EXAMPLE 41. Let $G = \{a_1, \cdots, a_n\}$ be a finite group. Let us define on it the function $\varphi_i(x)$ by supposing that $\varphi_i(a_j) = n\delta_{ij}$ where $\delta_{ii} = 1$ and $\delta_{ij} = 0$ for $i \neq j$. It is not hard to verify that the system $\varphi_i(x)$, $i = 1, \cdots, n$, is a complete orthonormal system of functions on the group G.

EXAMPLE 42. Let G^* be the additive topological group of real numbers, N the subgroup of all integers, and $G = G^*/N$. We have noted in Example 40 that every function defined on G can be treated as a periodic function of a real variable with period 1, and conversely. Let $\varphi_n(x) = e^{2\pi inx}$ be a function of the real variable x, where e is the base of natural logarithms, $i = \sqrt{-1}$, and n is an

* The proof of this theorem can be found in W. V. Lovitt's *Linear Integral Equations*, page 158, McGraw-Hill, New York, 1924.

integer. The function $\varphi_n(x)$ is of period 1 and hence can be regarded as defined on G. It can be shown in a straightforward way that the system $\varphi_n(x), n = 0, \pm 1, \pm 2, \cdots$ is an orthonormal system of functions defined on G. The completeness of this system follows from a well-known theorem of analysis, which we shall prove later (see Example 47).

27. Preliminary Remarks about Matrices

I shall review here a number of elementary propositions in the theory of matrices, and also give a proof of Schur's lemma which plays an important part in the theory of linear representations.

A) Let R be the r-dimensional vector space and f a linear transformation of R. The condition that the transformation f be linear may be expressed in the form

$$f(\alpha x + \beta y) = \alpha f(x) + \beta f(y) \tag{1}$$

where x and y are any two vectors of the space R and α and β are two real or complex numbers, according as R is a real or complex vector space.

Let $x_1, \cdots, x_r$ be the coordinates of the vector x in R, and $f_1(x), \cdots, f_r(x)$ the coordinates of $f(x)$. Then the following relations hold:

$$f_i(x) = \sum_{j=1}^{r} d_{ij} x_j, \tag{2}$$

where the coefficients d_{ij} do not depend on the choice of the vector x, but are defined by the transformation f. Hence for a fixed set of coordinates in the space R there exists a one-to-one correspondence between linear transformations of this space and square matrices of order r,

$$f \rightarrow \|d_{ij}\| = d. \tag{3}$$

If the transformation f is non-singular, then the determinant of the matrix $\|d_{ij}\|$ is not equal to zero, and conversely. The product of two transformations corresponds to the product of the corresponding matrices (see Example 2), and to the transformation f^{-1} inverse to f corresponds a matrix inverse to the matrix $\|d_{ij}\|$. The transformation f has an inverse if and only if the determinant of the corresponding matrix is not equal to zero.

The totality of all linear transformations, or of all the matrices whose determinants are different from zero, forms a group under multiplication. This group becomes topological in a natural way if we define an arbitrary neighborhood in it as the totality of all matrices $\|x_{ij}\|$ such that $|x_{ij} - a_{ij}| < \epsilon$, where $\|a_{ij}\|$ is a matrix with rational elements, and ϵ a positive rational number. Hence the topological group of matrices satisfies the second axiom of countability.

B) Let us replace the coordinates in R by a new set of coordinates, and let us suppose that the new and the old coordinates of the same vector are connected by the relation

(4) $$x_i = \sum_{j=1}^{r} t_{ij}x_j,$$

where the matrix $\|t_{ij}\| = t$ has a determinant different from zero. With this set of coordinates the transformation f will correspond to some matrix $\|d'_{ij}\| = d'$, where

(5) $$d' = tdt^{-1}.$$

We say that the matrix d is *transformed*, into the matrix d' by the matrix t. Hence the invariant properties of the transformation f are those and only those which belong simultaneously to all the matrices connected by relation (5). An example of such a property is afforded by the *trace* $s(d)$,

(6) $$s(d) = \sum_{i=1}^{r} d_{ii},$$

of the matrix d, since $s(d') = s(d)$. Hence we can talk about the trace of the transformation f and $s(f) = s(d)$. If a and b are two matrices, then the trace of their product does not depend on the order of the factors:

(7) $$s(ab) = s(ba).$$

C) Let the linear transformation f of the space R leave invariant some s-dimensional vector subspace S, $f(S) \subset S$, $0 < s < r$. Let us select a coordinate system in the space R in such a way that the first s axes lie in the space S. Then the matrix d which corresponds to the transformation f will be of the form

(8) $$d = \begin{Vmatrix} a & b \\ 0 & c \end{Vmatrix},$$

where a and c stand for square matrices of orders s and $r - s$, b is a rectangular matrix, and 0 is a rectangular matrix composed entirely of zeros. If d^* is the transpose of the matrix d (see Example 4), then the transformation f^* which corresponds to the matrix d^* leaves invariant a subspace generated by the last $r - s$ coordinate axes, and the dimensionality $r - s$ of this space is distinct from zero and from r. It is not true, however, that the connection between f and f^* is an invariant one. As a matter of fact this connection is purely accidental and depends on the choice of coordinates.

D) Let Δ be a set of linear transformations of the r-dimensional vector space R. The set Δ is called *reducible* if there exists an s-dimensional subspace S of the space R, with $0 < s < r$, which remains invariant under all the transformations of the set Δ. If this condition of reducibility is not satisfied, then Δ is called *irreducible*. We denote by Σ the set of all matrices which correspond to the transformations of the set Δ for a given set of coordinates. The set Σ of matrices will be called *reducible* or *irreducible* according as the set of transformations of Δ is reducible or not.

We shall show that if the set Σ of matrices is reducible, then the set Σ^* of the transposed matrices is also reducible.

It follows from C) that there exists a constant matrix t such that all the matrices $t\Sigma t^{-1}$ have the special form (8), i.e., if $x \varepsilon \Sigma$, then $txt^{-1} = x'$ has the form (8). By remark C) the matrix x'^* leaves invariant some subspace S' of the space R. Let us take the transpose of the relation $txt^{-1} = x'$ and solve it for x^*. We obtain $t^{*-1}x^*t^* = x'^*$, or $x^* = t^*x'^*t^{*-1}$. Since the matrix x'^* leaves invariant the subspace S', it follows that the matrix x^* also leaves invariant some subspace S'', and hence the family Σ^* of the matrices x^* is reducible.

We shall now prove the following important proposition due to I. Schur.

Schur's Lemma. *Let Σ and Ω be two irreducible sets of square matrices of orders m and n, and let a be a rectangular matrix of m rows and n columns such that*

$$\Sigma a = a\Omega, \tag{9}$$

i.e., *for every matrix $u \varepsilon \Sigma$ there exists a matrix $v \varepsilon \Omega$ such that*

$$ua = av, \tag{10}$$

and conversely, for every matrix $v' \varepsilon \Omega$ there exists a matrix $u' \varepsilon \Sigma$ such that

$$u'a = av'.$$

Under these conditions, only two cases are possible: either all the elements of the matrix a are equal to zero, or else $m = n$ and the square matrix a has a non-zero determinant.

Proof. Let R be the m-dimensional vector space with a certain coordinate system. Then the matrices of the set Σ can be regarded as linear transformations of the space R. Further let $a = \|a_{ij}\|$ and let a_k be the vector of the space R with coordinates $a_{1k}, \cdots, a_{mk}$. In this way the coordinates of the vector a_k are elements of the kth column of the matrix a. Let us denote by S a linear subspace of the space R generated by the vectors $a_1, \cdots, a_n$; we can then show that the subspace S is invariant under all transformations of the set Σ.

Let $u = \|u_{ij}\|$ be a matrix of the set Σ and $v = \|v_{ij}\|$ a matrix of the set Ω such that $ua = av$. Applying the transformation u to the vector a_k we get a vector b_k with coordinates $b_{ik} = \sum_{j=1}^{m} u_{ij}a_{jk}$, $i = 1, \cdots, m$. Calculating the corresponding member of the right side of the equality $ua = av$, we get $b_{ik} = \sum_{j=1}^{n} a_{ij}v_{jk}$, $i = 1, \cdots, m$. Hence the coordinates of the vector b_k are expressible as a linear combination of the coordinates of the vectors $a_1, \cdots, a_n$, which implies that $b_k \varepsilon S$. Hence all the transformations of the set Σ leave invariant the space S.

Since the set Σ is irreducible, the dimension of the space S must be zero or m. In the first case all the vectors a_k which generate the space S become zero, i.e., all the elements of the matrix a are zero. In the second case there are exactly m

linearly independent vectors in the system $a_1, \cdots, a_n$, which means that there are exactly m linearly independent columns in the matrix a. Therefore

$$n \geqq m. \tag{11}$$

Let us denote by Σ^* the set of matrices obtained by transposing the matrices of the set Σ, and by Ω^* the analogous set of matrices obtained from Ω. It follows from remark D) that the sets Σ^* and Ω^* are irreducible. We denote by a^* the transpose of the matrix a. Taking the transpose of relation (9) we get $\Omega^* a^* = a^* \Sigma^*$. Applying to this relation the same considerations that we applied to (9) we see that there are, as before, only two possibilities: either all the elements of the matrix a^* are zero, or else the matrix a^* contains n linearly independent columns. The first possibility has already been considered, while in the second case the matrix a contains n linearly independent rows, i.e., $n \leqq m$. This inequality combined with (11) proves that a is a square matrix whose determinant is different from zero, so that Schur's lemma is proved.

The following proposition is a direct consequence of Schur's lemma.

E) Let Ω be an irreducible set of square matrices of order r, and let b be a square matrix of order r which commutes with all the matrices of the set Ω. Then the matrix b has the form βe where β is a complex number and e is the unit matrix.

To prove this, let us consider the matrix $a = b - \beta e$, where β is a complex number chosen in such a way as to make the determinant of the matrix a equal to zero. Since the matrix b commutes with all matrices of the set Ω, the matrix a must possess the same property. We therefore have the relation $\Omega a = a\Omega$. It follows from the above lemma that all the elements of the matrix a are equal to zero, since the determinant of the matrix a is equal to zero by hypothesis. Hence $b = \beta e$.

F) Let Ω be an irreducible system of matrices such that any two of its matrices commute. Then all the matrices of the set Ω are of the first order.

It follows from E) that all the matrices of the set Ω are of the form βe, where β is a number, and e is the unit matrix. But a set of matrices of this form can be irreducible only if all the matrices are of the first order.

We shall pause here to discuss some special properties of unitary matrices.

G) Let R be a complex r-dimensional vector space, and x a vector with coordinates $x_1, \cdots, x_r$. Let us consider the Hermitian form

$$\varphi(x) = \sum_{i=1}^{r} x_i \bar{x}_i. \tag{12}$$

Let $d = \|d_{ij}\|$ be a matrix and f the transformation of the space R which corresponds to it. The matrix d is called *unitary* if the transformation f leaves invariant the Hermitian form (12), i.e. if $\varphi(f(x)) = \varphi(x)$ for every x. Straightforward calculations show that in order that the matrix d be unitary it is necessary and sufficient that the following relations hold:

$$\sum_{i=1}^{r} d_{ij}\bar{d}_{ik} = \delta_{jk}, \qquad (\delta_{ii} = 1,\ \delta_{ij} = 0 \text{ for } i \neq j). \tag{13}$$

Denoting by d^* the transpose of d, we can write (13) in the form

$$\bar{d}^* d = e \tag{14}$$

where e is the unit matrix. Hence d is unitary if and only if

$$d^{-1} = \bar{d}^*. \tag{15}$$

This last relation can be written in the form

$$d\bar{d}^* = e \tag{16}$$

or

$$\sum_{i=1}^{r} d_{ji}\bar{d}_{ki} = \delta_{jk}. \tag{17}$$

Relations (13) to (17) are equivalent and all express the unitary character of the matrix d. If the unitary matrix d is real, then it is orthogonal (see Example 4). We note that a unitary matrix leaves invariant not only the Hermitian form (12), but also the bilinear form $\psi(x, y) = \sum_{i=1}^{r} x_i \bar{y}_i$, where y is a vector with coordinates $y_1, \cdots, y_r$. We have in fact $\psi(f(x), f(y)) = \psi(x, y)$. If the bilinear form $\psi(x, y)$ of two vectors is equal to zero, then these vectors are called *orthogonal*. If the transformation f is unitary and if the vectors x and y are orthogonal, then the vectors $f(x)$ and $f(y)$ are also orthogonal.

H) Let R be the complex r-dimensional vector space, and x a vector with coordinates $x_1, \cdots, x_r$. Let us consider the Hermitian form

$$\varphi'(x) = \sum_{i=1}^{r} \sum_{j=1}^{r} a_{ij} x_i \bar{x}_j, \tag{18}$$

where the coefficients a_{ij} are symmetric, i.e.

$$a_{ij} = \bar{a}_{ji}. \tag{19}$$

The form (18) assumes only real values. Let us suppose that it is a positive definite form, i.e., it is always positive for $x \neq 0$. Let f be a transformation of the space R which leaves invariant the Hermitian form (18), i.e., $\varphi'(f(x)) = \varphi'(x)$. We denote the corresponding matrix by $d' = \|d'_{ij}\|$, and write $f \to d'$. As is well known we can reduce the positive definite Hermitian form (18) to the form (12) by a transformation of coordinates of the space R. In these new coordinates there corresponds to the transformation f a matrix $d = \|d_{ij}\|$. Hence $d = t^{-1}d't$, where d is a unitary matrix.

I) Let R be the r-dimensional complex vector space and f a unitary transformation with matrix $d = \|d_{ij}\|$. Let us suppose that f leaves invariant some s-dimensional space S, where $0 < s < r$. Let us denote by S' the space of all vectors orthogonal to every vector of the space S. Then S' is a space of $r - s$ dimensions. Let us select coordinates in the space R in such a way that the first s axes lie in the space S, while the remaining axes lie in the space S'.

In these new coordinates the matrix d' which corresponds to the transformation f has the special form

$$d' = \begin{Vmatrix} a & 0 \\ 0 & b \end{Vmatrix}$$

where $d' = tdt^{-1}$, and t, a, and b are unitary matrices.

J) It follows from the definition of a unitary matrix that the product of two unitary matrices is a unitary matrix, and that the matrix inverse to a unitary matrix is also unitary. Hence the set of all unitary matrices of order r forms a group G under multiplication. This group, being a subgroup of the topological group of all matrices whose determinants are different from zero, is topological (see A)). Since all the elements of a unitary matrix do not exceed one in absolute value by (13), the group G is compact. It is not hard to show that G satisfies the second axiom of countability (see A) and §12, B)). The set of all orthogonal matrices of order r forms a subgroup of the group G.

28. Orthogonality Relations

We shall denote here by G, as in §26, a compact topological group satisfying the second axiom of countability, and by $\bar{x}$ the complex conjugate of x.

Definition 32. A homomorphic mapping g of a topological group G in the topological group of matrices of order r (see §27, A)) is called a *representation of degree r* of the topological group G. In this way, to every element $x \in G$ corresponds a matrix $g(x)$ of order r whose elements we shall denote by $g_{ij}(x)$, $g(x) = \|g_{ij}(x)\|$. By a *representation* simply we mean a representation of some (unspecified) degree.

Two representations g and h of the group G of the same degree are called *equivalent* if there exists a constant matrix t (not depending on x) such that

$$h(x) = t^{-1}g(x)t \tag{1}$$

for every $x \in G$.

If g is a representation of a topological group G, $g(x) = \|g_{ij}(x)\|$, then the functions $g_{ij}(x)$ are continuous, since we have to do with a homomorphic mapping of one topological group in another, i.e., with a continuous mapping. Conversely, if there exists a homomorphic mapping g of an abstract group G in an abstract group of matrices, $g(x) = \|g_{ij}(x)\|$, and if the functions $g_{ij}(x)$ are continuous on the topological group G, then g is a homomorphic mapping of the topological group G in a topological group of matrices, i.e., g is a representation of the topological group G.

Theorem 23. *If g is a representation of the compact group G then there exists an equivalent representation g' all of whose matrices are unitary* (see §27, G)). *In other words for every representation there exists an equivalent unitary representation.*

PROOF. Let r be the degree of the representation g. Let us denote by R he r-dimensional complex vector space with a definite coordinate system, and et

$$\varphi(u) = \sum_{i=1}^{r} u_i\bar{u}_i, \tag{2}$$

where u is a vector in the space R with coordinates $u_1, \cdots, u_r$. To every natrix $g(x)$ corresponds some linear transformation of the space R, which we hall denote by g_x. We now substitute into the Hermitian form (2) the vecor $g_x(u)$ instead of the vector u and get

$$\varphi(g_x(u)) = \sum_{(i,j,k)=1}^{r} g_{ij}(x)\bar{g}_{ik}(x)u_j\bar{u}_k. \tag{3}$$

This new Hermitian form satisfies the condition of symmetry (19) of §27, and s positive definite (see §27, H)). We now construct a new Hermitian form

$$\varphi'(u) = \int \varphi(g_x(u))dx; \tag{4}$$

then $\varphi'(u)$ is also a positive definite form. We shall show that this form is invariant if we replace the vector u by the vector $g_y(u)$. To do this we substitute the vector $g_y(u)$ for u in (4), remembering that $g_x(g_y(u)) = g_{xy}(u)$ since g is a homomorphic mapping. Because of the invariance of integration (see Definition 31, 7)) we have

$$\varphi'(g_y(u)) = \int \varphi(g_{xy}(u))dx = \int \varphi(g_x(u))dx = \varphi'(u).$$

As we have already remarked (see §27, H)), the form $\varphi'(u)$ can be reduced to the form (12) of §27 by means of a transformation of coordinates in R. In these new coordinates to every transformation g_x will correspond the matrix $g'(x) = \|g'_{ij}(x)\|$, where $g'(x) = t^{-1}g(x)t$, and t is the matrix of the transformation of the coordinates. All the matrices $g'(x)$ are unitary and therefore the theorem is proved.

DEFINITION 33. The *character* $\chi(x)$ of the representation g of the group G is the trace of the matrix $g(x)$ (see §27, B)). Hence the character of a representation is a real valued function defined on G, namely $\chi(x) = s(g(x))$. Obviously, two equivalent representations have equal characters since the traces of the matrices $g(x)$ and $t^{-1}g(x)t$ are equal. The character of the representation is invariant, i.e.,

$$\chi(a^{-1}xa) = \chi(x), \tag{5}$$

where a is an arbitrary element of G. For

$$\chi(a^{-1}xa) = s(g(a^{-1}xa)) = s((g(a)^{-1}g(x)g(a)) = s(g(x)) = \chi(x).$$

A) Let g be a reducible representation of the group G. By Theorem 23 and remark I) of §27 we can assert that there exists a matrix t such that the matrices $h(x) = t^{-1}g(x)t$ have the special form

$$h(x) = \left\| \begin{matrix} g'(x) & 0 \\ 0 & g''(x) \end{matrix} \right\|,$$

where $g'(x)$ and $g''(x)$ are unitary matrices. We say then that the representation g decomposes into two representations g' and g''. If the representations g' and g'' are also reducible, then they in turn may be further decomposed. In this way every representation g can be decomposed into a finite system of irreducible representations $g_1, \cdots, g_n$. If we denote by $\chi(x)$ the character of the representation g and by $\chi_i(x)$ the character of the representation g_i, then the following equality holds

$$\chi(x) = \chi_1(x) + \cdots + \chi_n(x).$$

Theorem 24. *Let g and h be two distinct unitary irreducible non-equivalent representations of the group G, $g(x) = \|g_{ij}(x)\|$, $h(x) = \|h_{ij}(x)\|$. If we denote by $\chi(x)$ and $\chi'(x)$ the characters of the representations g and h, then the following orthogonality relations hold:*

$$\int g_{ij}(x)\bar{h}_{kl}(x)dx = 0, \tag{6}$$

$$\int \chi(x)\bar{\chi}'(x)dx = 0. \tag{7}$$

Proof. Let m be the degree of the representation g, and n be the degree of the representation h. Let us denote by b a constant matrix with m rows and n columns, and let $a(x) = g(x)bh(x^{-1})$. Let $a = \int a(x)dx$. It is not hard to show that $g(y)ah(y^{-1}) = a$. In fact

$$g(y)ah(y^{-1}) = \int g(y)g(x)bh(x^{-1})h(y^{-1})dx = \int g(yx)bh((yx)^{-1})dx = a$$

(see Definition 31, 8)). We have, therefore, $g(x)a = ah(x)$. It follows from Schur's Lemma (see §27) that there are two possible cases. If we suppose that the determinant of the matrix a is different from zero, we get $h(x) = a^{-1}g(x)a$, i.e., the representations g and h are equivalent, which contradicts the assumption of the theorem. Therefore, the matrix a is composed of zeros and we have

$$\int g(x)bh(x^{-1})dx = a = 0.$$

Let us select the matrix b in a special way by supposing that its element in the j-th row and l-th column is unity, while all the other elements are equal to zero. Then, by taking into consideration relation (15) of §27 we obtain

$$\int g_{ij}(x)\bar{h}_{kl}(x)dx = 0.$$

Relation (7) for the characters $\chi(x)$ and $\chi'(x)$ follows from (6) since $\chi(x)$ and $\chi'(x)$ can be expressed in terms of $g_{ii}(x)$ and $h_{jj}(x)$.

THEOREM 25. *Let g be a unitary irreducible representation of the group G of degree r, $g(x) = \|g_{ij}(x)\|$. Let us denote the character of the representation g by*

$$\chi(x) = \sum_{i=1}^{r} g_{ii}(x). \tag{8}$$

Then the following orthogonality relations hold:

$$\int g_{ij}(x)\bar{g}_{ij}(x)dx = \frac{1}{r} \cdot \tag{9}$$

If $i \neq k$ or $j \neq l$ then

$$\int g_{ij}(x)\bar{g}_{kl}(x)dx = 0, \tag{10}$$

and finally

$$\int \chi(x)\bar{\chi}(x)dx = 1. \tag{11}$$

PROOF. Let us denote by $b = \|b_{ij}\|$ a constant square matrix of order r, and let $a(x) = g(x)bg(x^{-1})$ and $a = \int a(x)dx$. It is not hard to see that the matrix a has the following property of invariance

$$g(y)ag(y^{-1}) = a. \tag{12}$$

In fact

$$g(y)ag(y^{-1}) = \int g(y)g(x)bg(x^{-1})g(y^{-1})dx = \int g(yx)bg((yx)^{-1})dx = a$$

(see Definition 31, 8)). It follows from relation (12) that $g(x)a = ag(x)$ for an arbitrary x. From this together with remark E) of §27 we can conclude that the matrix a is of the form $\alpha e'$, where e' is the unit matrix and α is a complex number depending on the matrix b. Hence

$$\int g(x)bg(x^{-1})dx = \alpha e'. \tag{13}$$

Let us determine the number α. To do this we take the trace of both sides of relation (13). Taking into consideration formulas (15) and (13) of §27 we have

$$s\left(\int g(x)bg(x^{-1})dx\right) = \int \sum_{(i,j,k)=1}^{r} g_{ij}(x)b_{jk}\bar{g}_{ik}(x)dx = \int \sum_{(j,k)=1}^{r} \delta_{jk}b_{jk}dx$$

$$= \int \sum_{j=1}^{r} b_{jj}dx = s(b).$$

But the trace of the right hand side of (13) is equal to αr, and therefore $\alpha = s(b)/r$.

Let us now select the matrix b in a special way by supposing that only the element standing in the j-th row and l-th column is distinct from zero, and that this element is equal to unity. Then $s(b) = \delta_{jl}$. Making use of formula (15) of §27, we get under these conditions from relation (13),

$$\int g_{ij}(x)\bar{g}_{kl}(x)dx = \frac{1}{r}\,\delta_{ik}\delta_{jl}. \tag{14}$$

But the last relation is equivalent to (9) and (10), and from it also follows relation (11). Hence the theorem is proved.

We now consider in greater detail the characters of the representations.

B) Let Δ be the set of characters of all the inequivalent irreducible representations of the group G. It follows from (7) and (11) that Δ is an orthonormal system of functions defined on G. Hence Δ contains not more than a countable number of functions (see Theorem 22) and we can suppose

$$\Delta = \{\chi_1(x), \cdots, \chi_r(x), \cdots\}.$$

Let g be a representation of the group G and $\chi(x)$ its character. By A) the representation g decomposes into a system of irreducible representations and we have

$$\chi(x) = \sum_{i=1}^{n} m_i\chi_i(x), \tag{15}$$

where m_i is a non-negative integer denoting the multiplicity with which the irreducible representation g_i of character $\chi_i(x)$ occurs in the representation g. Multiplying (15) by $\bar{\chi}_k(x)$ and integrating we get

$$m_k = \int \chi(x)\bar{\chi}_k(x)dx.$$

Hence the numbers m_k are the Fourier coefficients of the function $\chi(x)$ with respect to the system Δ. This means that the numbers m_k are uniquely determined by the function $\chi(x)$. Hence the character $\chi(x)$ of the representation g determines g uniquely up to equivalence.

Multiplying (15) by its conjugate and integrating we get

$$\sum_{i=1}^{n} m_i^2 = \int \chi(x)\bar{\chi}(x)dx. \tag{16}$$

The last relation gives us a criterion for the irreducibility of the representation g, namely, a representation g is irreducible if and only if its character $\chi(x)$ satisfies the condition

$$\int \chi(x)\bar{\chi}(x)dx = 1. \tag{17}$$

If the representation g is reducible, then

$$\int \chi(x)\bar{\chi}(x)dx > 1.$$

THEOREM 26. *If the group G is commutative then all its irreducible representations are of the first degree, and every irreducible representation g coincides with its character $\chi(x)$, $g(x) = \|\chi(x)\|$, since the matrix $g(x)$ reduces in this case to an ordinary number.*

The proof follows directly from remark F) of §27.

EXAMPLE 43. Let G and H be two compact topological groups satisfying the second axiom of countability. Let us denote by F their direct product. Every element z of F represents a pair (x, y), where $x \in G$, $y \in H$. Let g and h be irreducible representations of the groups G and H of degrees m and n respectively, $g(x) = \|g_{ij}(x)\|$, $h(y) = \|h_{kl}(y)\|$. From the representations g and h of the groups G and H we construct a representation f of the group F which is also irreducible. To do this we introduce a double index (i, k), where the first element of the pair runs over the values $1, \cdots, m$ and the second the values $1, \cdots, n$. It is of course possible to number all pairs (i, k) with the numbers $1, \cdots, mn$, but we shall not make use of that. We now introduce a new square matrix $f(z) = \|f_{(i,k)(j,l)}(z)\|$ of order mn by letting $f_{(i,k)(j,l)}(z) = g_{ij}(x)h_{kl}(y)$, where $z = (x, y)$. It is not hard to verify that the matrix $f(z)$ gives a representation of the group F. We shall show that this representation is irreducible. To do this we calculate the character $\chi(z)$ of the representation f. We denote by $\chi'(x)$ and $\chi''(y)$ the characters of the representations g and h. Direct calculations show that $\chi(z) = \chi'(x)\chi''(y)$, where $z = (x, y)$. Applying to the character $\chi(z)$ the criterion of irreducibility (17) we obtain

$$\int \chi(z)\bar{\chi}(z)dz = \int\int \chi'(x)\chi''(y)\bar{\chi}'(x)\bar{\chi}''(y)dxdy = 1$$

(see proof of Theorem 21). Hence the representation f is irreducible. In the next section we shall show that all irreducible representations of the group F can be obtained by a similar construction—of course, only up to an equivalence (see Example 45).

EXAMPLE 44. Let G be the topological group discussed in Examples 40 and 42, and $\varphi_n(x)$, $n = 0, \pm 1, \pm 2, \cdots$ the system of functions defined on G in Example 42, $\varphi_n(x) = e^{2\pi i n x}$. Let us consider the matrix of the first order

$g_n(x) = \|\varphi_n(x)\|$. Then g_n is a representation of the group G of the first degree, and moreover, g_n is unitary. The character of the representation g_n is the function $\varphi_n(x)$. Since the functions $\varphi_n(x)$, $n = 0, \pm 1, \pm 2, \cdots$, form a complete orthogonal system in G, there exist no irreducible representations of the group G besides the representations g_n which we have just constructed, for in the contrary case the complete system of orthogonal functions could be enlarged by one more function, orthogonal to all the others, which is impossible.

29. The Completeness of the System of Irreducible Representations

In the present section we give an exposition of the results of Peter and Weyl concerning the completeness of the system of functions arising from irreducible representations. The proof given here differs from the original proof (see [29]) inasmuch as we make use of the orthogonality of the system in proving its completeness, which simplifies the proof greatly.

Here, as in the preceding section, we designate by G a compact topological group satisfying the second axiom of countability. All the functions considered here are continuous.

THEOREM 27. *We select from each class of mutually equivalent irreducible representations of the group G a unitary representation. By remark* B) *of* §28 *there is only a countable number of such representations which we number by writing them as*

$$(1) \qquad \overset{(1)}{g}, \cdots, \overset{(n)}{g}, \cdots, \qquad \overset{(n)}{g}(x) = \|\overset{(n)}{g_{ij}}(x)\|.$$

We denote by Δ *the totality of all functions* $\overset{(n)}{g_{ij}}(x)$ *arising from the representations of the system* (1). *Then the system* Δ *is a uniformly complete system of functions on* G (see §26, D)), *and hence from relations* (6), (9), *and* (10) *of* §28, *and from Theorems* 24 *and* 25, *the system* Δ *is a complete orthogonal system of functions of* G (see §26, E)).

PROOF. Let $k(z)$ be a real continuous function defined on G which satisfies the condition of symmetry

$$(2) \qquad k(z^{-1}) = k(z).$$

Let us consider the integral equation

$$(3) \qquad \varphi(x) = \lambda \int k(x^{-1}y)\varphi(y)dy.$$

It follows from (2) that the kernel of equation (3) is symmetric,

$$k(x^{-1}y) = k(y^{-1}x).$$

We denote by Δ' the totality of all characteristic functions of all the equations of type (3) (see §26, G)) and show that the system of functions Δ' is a uniformly complete system on G.

Let $f(x)$ be a continuous function defined on G. Since the function $f(x)$ is

continuous it is uniformly continuous (see §24, C)), i.e., for every positive ϵ there exists a neighborhood U of the identity e of the group G such that for $x^{-1}y \varepsilon U$ we have

$$(4) \qquad |f(x) - f(y)| < \tfrac{1}{2}\epsilon$$

and $U^{-1} = U$. Let V be a neighborhood of the identity e such that $\bar{V} \subset U$. By Urysohn's Lemma (see §14) there exists a continuous function $q(z)$ such that $0 \leqq q(z) \leqq 1$ for every $z \varepsilon G$, $q(z) = 0$ for $z \varepsilon G - U$ and $q(z) = 1$ for $z \varepsilon \bar{V}$. Let $k'(z) = \alpha(q(z) + q(z^{-1}))$, where α is a real positive number selected in such a way that $\int k'(z)dz = 1$. The function $k'(z)$ is different from zero only for $z \varepsilon U$ and satisfies the condition of symmetry (2). Let

$$f'(x) = \int k'(x^{-1}y)f(y)dy.$$

Because of the special choice of the function $k'(z)$ and inequality (4) we have

$$(5) \qquad |f(x) - f'(x)| < \tfrac{1}{2}\epsilon.$$

In fact

$$|f'(x) - f(x)| = \left|\int k'(x^{-1}y)(f(y) - f(x))dy\right| \leqq \int k'(x^{-1}y)\cdot\tfrac{1}{2}\epsilon dy = \tfrac{1}{2}\epsilon.$$

By remark I) of §26 the function $f'(x)$ can be decomposed into a uniformly convergent series

$$f'(x) = \varphi_1(x) + \cdots + \varphi_n(x) + \cdots,$$

where the functions $\varphi_i(x)$, $i = 1, 2, \cdots$, are characteristic functions of the equation

$$(6) \qquad \varphi(x) = \lambda \int k'(x^{-1}y)\varphi(y)dy.$$

Therefore there exists an n sufficiently large so that the function

$$(7) \qquad f''(x) = \sum_{i=1}^{n} \varphi_i(x)$$

satisfies the inequality

$$(8) \qquad |f'(x) - f''(x)| < \tfrac{1}{2}\epsilon.$$

Combining inequalities (5) and (8) we get

$$(9) \qquad |f(x) - f''(x)| < \epsilon.$$

Since equation (6) is of the form (3), all the functions $\varphi_i(x)$, $i = 1, \cdots, n$, belong to the system Δ'. But since ϵ is arbitrarily small, the uniform completeness of the system Δ' follows from (7) and (9).

Let us denote by Δ'' the set of all functions $g_{ij}(x)$ arising from all possible representations g, $g(x) = \|g_{ij}(x)\|$, of the group G and let us show that the system of functions Δ'' is uniformly complete in G.

To prove this it is sufficient to show that every function of the system Δ' can be expressed as a finite linear form in the functions of the system Δ'' with constant coefficients, since the uniform completeness of the system Δ' has already been shown.

If $\varphi'(x)$ is a function of the system Δ' it satisfies equation (3) for some choice of the kernel $k(z)$. Let λ' be that characteristic value of the parameter λ to which corresponds the function $\varphi'(x)$. We denote by

$$\varphi_1(x), \cdots, \varphi_n(x) \tag{10}$$

the complete orthogonal system of solutions of equation (3) which belong to the given characteristic value λ' (see §26, H)). Then $\varphi'(x)$ can be expressed as a linear combination of functions of the system (10), and it will suffice to show that every function of the system (10) can be expressed as a linear combination of functions of the system Δ''.

If the function $\varphi(x)$ is a solution of equation (3), then the function $\varphi(ax)$ is also a solution of (3) for the same characteristic value λ. In fact since x is an arbitrary variable in equation (3), x can be replaced by ax, and at the same time, because of the invariance of integration, y can be replaced by ay, and we get

$$\varphi(ax) = \lambda \int k(x^{-1}a^{-1}ay)\varphi(ay)dy = \lambda \int k(x^{-1}y)\varphi(ay)dy.$$

Therefore, the functions

$$\varphi_1(ax), \cdots, \varphi_n(ax) \tag{11}$$

are solutions of equation (3) for the characteristic value λ', and hence can be expressed as a linear combination of functions of the system (10). In this way we obtain

$$\varphi_i(ax) = \sum_{j=1}^{n} g_{ij}(a)\varphi_j(x). \tag{12}$$

Moreover, the system (11) is orthogonal, since

$$\int \varphi_i(ax)\varphi_j(ax)dx = \int \varphi_i(x)\varphi_j(x)dx = \delta_{ij}.$$

Hence the functions of the system (11) are linearly independent, and the functions of the system (10) can be expressed as linear combinations of them. Hence the matrix $\|g_{ij}(x)\| = g(x)$ has an inverse. It could also be shown that the matrix $g(x)$ is orthogonal, but this is not essential for our purposes. We

shall show that the functions $g_{ij}(x)$ are continuous. In fact multiplying (12) by $\varphi_k(x)$ and integrating we get

$$g_{ik}(a) = \int \varphi_i(ax)\varphi_k(x)dx$$

(see §25, J)). We next calculate $g(ab)$. We have from (12),

$$\varphi_i(abx) = \sum_{j=1}^{n} g_{ij}(ab)\varphi_j(x). \tag{13}$$

From the same relation (12) we also get

$$\varphi_i(abx) = \sum_{k=1}^{n} g_{ik}(a)\varphi_k(bx) = \sum_{(k,j)=1}^{n} g_{ik}(a)g_{kj}(b)\varphi_j(x). \tag{14}$$

Comparing coefficients in the right sides of (13) and (14) we get

$$g_{ij}(ab) = \sum_{k=1}^{n} g_{ik}(a)g_{kj}(b),$$

which can be written in matrix form

$$g(ab) = g(a)g(b). \tag{15}$$

It follows from (15) and from the continuity of the functions $g_{ij}(x)$ that $g(x)$ gives a representation of the group G, and therefore all the functions

$$g_{ij}(x) \tag{16}$$

belong to the system Δ''.

We now replace x in equation (12) by the identity e. We obtain

$$\varphi_i(a) = \sum_{j=1}^{n} g_{ij}(a)\varphi_j(e).$$

But this means that the functions of the system (10) are expressed as a linear combination of functions of the system (16) belonging to the system Δ''. This proves that the system Δ'' is uniformly complete.

All the functions of the system Δ appear in the system Δ'', $\Delta \subset \Delta''$. We shall now show that every function of the system Δ'' is expressible as a linear combination of functions of the system Δ. This will show that the system Δ is uniformly complete, since the uniform completeness of the system Δ'' has already been proved.

Let $p(x)$ be an arbitrary function of the system Δ''. Then there exists a representation g of the group G, $g(x) = \|g_{ij}(x)\|$, such that $p(x)$ is one of the functions

$$g_{ij}(x). \tag{17}$$

By remark A) of §28 there exists a constant matrix t such that

$$g(x) = t^{-1}h(x)t, \tag{18}$$

where the matrix $h(x)$ has the special form

$$h(x) = \begin{vmatrix} g_1(x) & 0 & \cdots & 0 \\ 0 & g_2(x) & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & g_n(x) \end{vmatrix}$$

and where

$$g_i(x),\ i = 1, 2, \cdots, n, \tag{19}$$

give irreducible unitary representations of the group G. By a special choice of the matrix t it is possible to have all the representations of the system (19) belong to the system (1), for the system (1) contains irreducible representations equivalent to any given representation. If we then suppose that the representations (19) belong to the system (1), then relation (18) shows that all the functions (17) can be expressed as linear combinations of functions of the system Δ. In particular, this is true for the function $p(x)$. Hence the uniform completeness of the system Δ is established.

The following proposition, which plays a particularly important part in the study of compact topological groups, is a direct consequence of Theorem 27.

THEOREM 28. *We select one representative from each class of irreducible equivalent representations of the group G and denote the representatives by*

$$g^{(1)}, \cdots, g^{(n)}, \cdots. \tag{20}$$

Then for every element $a \in G$ distinct from the identity, there exists a representation $g^{(m)}$ of the system (20) *such that $g^{(m)}(a)$ is not the unit matrix.*

PROOF. It follows from Urysohn's Lemma that since $a \neq e$, there exists a function $f(x)$ defined on G such that $f(a) \neq f(e)$ (see §14). If, contrary to the statement of the theorem, the equality $g^{(n)}(a) = g^{(n)}(e)$, should hold for every representation $g^{(n)}$ of the system (20), then we should have for every function of the system Δ (see Theorem 27) the equality $g^{(n)}_{ij}(a) = g^{(n)}_{ij}(e)$. But in this case it would be impossible to approximate the function $f(x)$ by linear forms in the functions of the system Δ, since $f(a) \neq f(e)$. Hence Theorem 28 is established.

We now pass to the consideration of systems of characters.

THEOREM 29. *Let*

$$\Omega = \{\chi_1(x), \cdots, \chi_n(x), \cdots\}$$

be the totality of all characters of irreducible representations of the group G. We shall say that the function $f(x)$ defined on G is invariant if

$$f(a^{-1}xa) = f(x) \tag{21}$$

for every $a \varepsilon G$. From relation (5) of §28 the functions of the system Ω are invariant. The assertion of this theorem is that the system Ω is uniformly complete with respect to all invariant functions defined on G. This means that for every invariant function $f(x)$ defined on G, and for every positive ϵ, there exists a linear form $f'(x) = \sum_{i=1}^{n} c_i\chi_i(x)$ with constant coefficients such that

$$|f(x) - f'(x)| < \epsilon.$$

PROOF. Let g be an irreducible representation of the group G of degree r, $g(x) = \| g_{ij}(x)\|$. Let us suppose that the function

$$p(x) = \sum_{(i,j)=1}^{r} b_{ji}g_{ij}(x) \tag{22}$$

is invariant. We can then show that

$$p(x) = \alpha\chi(x) \tag{23}$$

where $\chi(x)$ is the character of the representation g, and α is a number.

By assumption

$$p(a^{-1}xa) = \sum_{(i,j)=1}^{r} b_{ji}g_{ij}(a^{-1}xa) = \sum_{(j,i,k,l)=1}^{r} b_{ji}g_{ik}(a^{-1})g_{kl}(x)g_{lj}(a) = p(x). \tag{24}$$

Since all the functions $g_{ij}(x)$ are linearly independent (see Theorems 23 and §26, F)), the corresponding coefficients b in (22) and (24) must be equal and we have

$$b_{lk} = \sum_{(i,j)=1}^{r} g_{lj}(a)b_{ji}g_{ik}(a^{-1}).$$

In matrix notation this last equality can be written: $b = g(a)bg(a^{-1})$, where $b = \|b_{ij}\|$; it can also be written $g(a)b = bg(a)$. From remark E) of §27 we can conclude from this that the matrix b has the form $\alpha e'$, where e' is the unit matrix, and α is a number. Then equation (22) assumes the form (23).

Now let $q(x)$ be an invariant function defined on G which is expressible as a finite linear form in the functions of Δ (see Theorem 27). The sum $q(x)$ can be decomposed into a series of partial sums $p_i(x)$, $q(x) = \sum_{i=1}^{n} p_i(x)$, where each sum $p_i(x)$ has the form (22), i.e., it is composed of functions belonging to one irreducible representation $g^{(i)}$. It follows from the invariance of the function $q(x)$ that each of the functions $p_i(x)$ is also invariant. For the function $p_i(a^{-1}xa)$ can be expressed as a function of x linearly in terms of the functions $g_{kl}^{(i)}(x)$ belonging to the representation $g^{(i)}$ (see equation (24)). It follows from this and from the linear independence of the functions of the system Δ, that the equation

$$\sum_{i=1}^{n} p_i(a^{-1}xa) = \sum_{i=1}^{n} p_i(x)$$

must be true termwise, i.e., $p_i(a^{-1}xa) = p_i(x), i = 1, \cdots, n$. We therefore obtain from (23) the equation $p_i(x) = \alpha_i\chi_i(x)$, i.e.,

$$q(x) = \sum_{i=1}^{n} \alpha_i\chi_i(x). \tag{25}$$

Finally let $f(x)$ be an arbitrary invariant function defined on G. By Theorem 27 there exists a finite linear form $f'(x)$ of functions of the system Δ such that

$$|f(x) - f'(x)| < \epsilon, \tag{26}$$

where ϵ is a preassigned positive number. It follows from inequality (26) that

$$\left|\int f(a^{-1}xa)da - \int f'(a^{-1}xa)da\right| < \epsilon. \tag{27}$$

Since $f(x)$ is invariant we have $\int f(a^{-1}xa)da = f(x)$. Let us suppose that $\int f'(a^{-1}xa)da = q(x)$. Then inequality (27) has the form

$$|f(x) - q(x)| < \epsilon.$$

Since the function $f'(x)$ is a finite linear form in the functions of the system Δ, $f'(a^{-1}xa)$ has the same form as a function of x, and therefore $q(x)$ is a finite linear form in the functions of the system Δ. It is not hard to see that the function $q(x)$ is invariant, because of the invariance of integration (see Definition 31, 7)). It follows from relation (25) that $q(x) = \sum_{i=1}^{n}\alpha_i\chi_i(x)$. Hence $|f(x) - \sum_{i=1}^{n}\alpha_i\chi_i(x)| < \epsilon$ and the theorem is proved.

A) Let

$$\Omega = \{\chi_1(x), \cdots, \chi_n(x), \cdots\}$$

be the totality of all characters of irreducible representations of the group G and $f(x)$ an invariant function defined on G. We denote by h_i the Fourier coefficients of the function $f(x)$ with respect to the system Ω,

$$h_i = \int f(x)\bar{\chi}_i(x)dx.$$

Then we have the equation

$$\sum_{i=1}^{\infty} h_i\bar{h}_i = \int f(x)\bar{f}(x)dx.$$

The proof is based on Theorem 29, and is analogous to the proof of Remark E) of §26.

Just as Theorem 28 follows from Theorem 27, so Theorem 30 can be made to follow directly from Theorem 29. This theorem is, however, not important for our purposes.

Theorem 30. *Let a and b be two non-conjugate elements of the group G, i.e., elements such that there exist no element $c \varepsilon G$ for which $b = c^{-1}ac$. Then there exists a character $\chi(x)$ of an irreducible representation of the group G such that $\chi(a) \neq \chi(b)$.*

Proof. It is not hard to see that the set B of all elements conjugate to b is compact. From Urysohn's Lemma (see §14) there exists a non-negative function $f(x)$ which is zero on B and different from zero at a. Moreover the function $\varphi(x) = \int f(y^{-1}xy)dy$ is invariant, and $\varphi(b) = 0$, while $\varphi(a) \neq 0$. By Theorem 29 the function $\varphi(x)$ can be approximated uniformly by means of linear forms in functions of the system Ω (see A)), and hence there exists a function in Ω which assumes distinct values at the points a and b.

Example 45. Let us complete the discussion of Example 43. Let

$$\Omega' = \{\chi'_1(x), \quad \cdots, \chi'_n(x), \cdots\}$$

be the totality of all the characters of irreducible representations of the group G and let

$$\Omega'' = \{\chi''_1(y), \cdots, \chi_n''(y), \cdots\}$$

be the totality of all the characters of irreducible representations of the group H. Let us denote by Ω the totality of all the functions $\chi_{ij}(z) = \chi'_i(x)\chi''_j(y)$ where $z = (x, y)$. It follows from what we have shown in Example 43 that all the functions of the system Ω are characters of irreducible representations of the group F. We shall show now that the system Ω contains all the characters of the irreducible representations of the group F.

Let $f(z) = f(x, y)$ be an invariant function defined on F. Let us determine the Fourier coefficients of this function with respect to the system Ω by setting

$$f_{ij} = \int f(z)\bar{\chi}_{ij}(z)dz = \int\int f(x, y)\bar{\chi}'_i(x)\bar{\chi}''_j(y)dxdy \tag{28}$$

(see proof of Theorem 21). The function $f(x, y)$ is an invariant function on H for a fixed x. Let us determine its Fourier coefficients with respect to the system Ω'' by setting

$$f_j(x) = \int f(x, y)\bar{\chi}''_j(y)dy.$$

From remark A) we have

$$\sum_{j=1}^{\infty} f_j(x)\bar{f}_j(x) = \int f(x, y)\bar{f}(x, y)dy. \tag{29}$$

The series on the left side of equation (29) is composed of positive continuous functions and converges to a continuous function; therefore, by a well known

theorem of analysis, it is uniformly convergent and we can integrate it termwise. We then obtain

$$(30) \qquad \sum_{j=1}^{\infty} \int f_j(x)\bar{f}_j(x)dx = \int\int f(x, y)\bar{f}(x, y)dxdy.$$

It can readily be seen that the function $f_j(x)$ defined on G is continuous and invariant. Determining its Fourier coefficients with respect to the system Ω' we get

$$\int f_j(x)\bar{\chi}_i(x)dx = f_{ij}.$$

But from A) we have

$$(31) \qquad \int f_j(x)\bar{f}_j(x)dx = \sum_{i=1}^{\infty} f_{ij}\bar{f}_{ij}.$$

Combining relations (30) and (31) we get

$$(32) \qquad \sum_{(i,j)=1}^{\infty} f_{ij}\bar{f}_{ij} = \int\int f(x, y)\bar{f}(x, y)dxdy = \int f(z)\bar{f}(z)dz.$$

Let us now suppose that some character $\chi(z)$ of an irreducible representation of the group F does not belong to the system Ω. Then all the Fourier coefficients of the function $\chi(z)$ with respect to the system Ω will be equal to zero (see Theorem 24). But on the other hand by Theorem 25, $\int\chi(z)\bar{\chi}(z)dz = 1$. Hence we have arrived at a contradiction to equation (32) for the function $f(z) = \chi(z)$.

Therefore the construction given in Example 43 gives all possible irreducible representations of the direct product F by starting with irreducible representations of its factors G and H.

Example 46. We give here an application of the theory of representations to the theory of almost periodic functions.

A continuous complex function $f(t)$ of a real variable t, $-\infty < t < +\infty$, is called *almost periodic* if the family H of all functions of the form $f(t + a)$, where a is an arbitrary real number, is compact, i.e., if from any sequence $f(t + a_1), \cdots, f(t + a_n), \cdots$ there can be selected a uniformly convergent subsequence.

The simplest example of almost periodic functions are the periodic functions of the form $e^{i\lambda t}$, where λ is an arbitrary real number, and $i = \sqrt{-1}$. We denote the set of all functions of the form $e^{i\lambda t}$ by Δ. We shall show that the system Δ is uniformly complete in the set of all almost periodic functions (see §26, D)). This proposition is the fundamental theorem in the theory of almost periodic functions.

Starting with a definite almost periodic function $f(t)$, we denote by G the set of all functions which are uniform limits of functions of the family H. The

set G is compact in the sense of uniform convergence, and is a topological space satisfying the second axiom of countability. The set H is everywhere dense in G. We define addition in the set H as follows: if $x' = f(t + a')$ and $x'' = f(t + a'')$ are two elements of the set H, then their sum $x' + x''$ is defined as the function $f(t + a' + a'')$, also belonging to the family H. The operation of addition thus defined in the set H can be uniquely extended to all elements of the set G because of continuity. In this way G becomes a compact commutative topological group, satisfying the second axiom of countability. Therefore to the group G is applicable all of the theory of representations.

Let

$$g^{(1)}, \cdots, g^{(n)}, \cdots \tag{33}$$

be the totality of all irreducible representations of the group G. Since, by Theorem 26, all irreducible representations of the group G are of degree 1, it follows that $g^{(n)}$ is simply a homomorphic mapping of the group G into the multiplicative group K of complex numbers of absolute value unity. Hence $g^{(n)}(x)$ is a complex number of absolute value unity, and

$$g^{(n)}(x + y) = g^{(n)}(x)g^{(n)}(y). \tag{34}$$

If x belongs to the subset H, then x is a function of the form $f(t + a)$ and therefore depends on the parameter a. We therefore write $x = x(a)$, and we have from the addition defined in H that $x(a') + x(a'') = x(a' + a'')$. It can readily be seen, moreover, that as an element of the space G, $x(a)$ is a continuous function of the parameter a. We shall now consider the meaning of $g^{(n)}(x(a))$. We have

$$g^{(n)}(x(a' + a'')) = g^{(n)}(x(a'))g^{(n)}(x(a'')).$$

Hence if we consider $g^{(n)}(x(a))$ as a function of the parameter a, then $g^{(n)}(x(a))$ gives a homomorphic mapping of the additive group of real numbers in the group K. We can conclude from this that $g^{(n)}(x(a)) = e^{i\lambda_n a}$ since every homomorphism of the type indicated is expressible in this form (see §32, H)).

We associate with every element $x(a) \in H$ the number $f'(x) = f(a)$. In this way we have defined the function $f'(x)$ on H. This function can be extended by continuity to the whole group G, and will be continuous on G.

By Theorem 27 the function $f'(x)$ can be uniformly approximated by finite linear forms in the functions (33). If we consider this approximation only on H, we obtain an approximation of the function $f(a)$ by linear forms in the functions $g^{(n)}(x(a)) = e^{i\lambda_n a}$, $n = 1, 2, \cdots$. Hence the system Δ is uniformly complete in the set of all almost periodic functions.

CHAPTER V

COMMUTATIVE TOPOLOGICAL GROUPS

The present chapter is devoted to the detailed investigation of locally compact topological commutative groups satisfying the second axiom of countability. All the questions arising here are completely solved or are at least reduced to questions concerning abstract commutative groups.

The principal method employed in this chapter consists in the construction of a character group (see Definition 34). To every locally compact topological commutative group G satisfying the second axiom of countability there corresponds a locally compact topological commutative group X satisfying the second axiom of countability, which is called the character group of the group G. The correspondence thus established between the groups G and X is symmetric. It enables us to reduce any question concerning one of these groups to the corresponding question about the other.

If the group G is compact then its character group X is discrete, and conversely (see §17, A)). In this way the study of compact commutative groups is reduced to the study of discrete, or what is the same, abstract groups. The structure of locally compact groups is made quite clear.

The main results depend on the theory of representations of Peter and Weyl. We have already shown in the previous chapter (see Theorem 26) that every irreducible representation of a commutative group G is a representation of the first degree, i.e., it essentially coincides with the character of the representation. It now appears that the totality of all characters of the group G forms in a natural way a new group X, which is called the character group of G. Let us consider this in greater detail. Let $g(x)$ be a unitary irreducible representation of the group G. Since it is of the first degree, we can say simply that $g(x)$ is a complex number of absolute value unity. In other words $g(x)$ can be considered as a homomorphic mapping of the group G into the multiplicative group of complex numbers of absolute value unity. If $g(x)$ and $h(x)$ are two such mappings, then $f(x) = g(x)h(x)$ is also a mapping of the same type. It is in this way that we define the operation of multiplication in a character group.

The fundamental results of this chapter are due to myself (see [27], [28], and [25]). A number of important generalizations and improvements obtained by van Kampen (see [13] and [15]) will also be taken into account.

All the topological groups considered in this chapter are commutative, locally compact, and satisfy the second axiom of countability. These conditions are always supposed to be satisfied, even if they are not explicitly stated.

Since all the groups discussed here are commutative we shall use the additive notation. Therefore, the multiplicative group of complex numbers of absolute value one will be replaced by an additive group K isomorphic with it, whose complete definition will be given at the beginning of §30. Since this group will

play a fundamental part in the whole discussion, the letter K will be reserved for it during the whole chapter.

30. Character Groups

We shall first of all construct a character group (see Definition 34) and then give a proof of its simplest fundamental properties (see Theorem 31).

A) Let D be the additive topological group of real numbers, and N its subgroup of all integers. We denote by K the factor group D/N (see Definition 25). It can readily be seen that K is a compact topological group satisfying the second axiom of countability. Since the group K arises from the group of real numbers, we shall sometimes treat its elements as real numbers defined up to an additive integer. If, in particular, we limit ourselves to the consideration of a sufficiently small neighborhood U of zero of the group K, then we can assign uniquely and continuously to each of its elements a definite numerical value, taking for the numerical value of an element $a \varepsilon U$ the least real number (in absolute value) from which the element a has arisen.

Definition 34. Let G be a locally compact commutative topological group satisfying the second axiom of countability. Every homomorphic mapping of the group G in the group K (see A)) will be called a *character* of the group G. The set of all characters of the group G we denote by X. We can introduce n a natural way into the set X an operation of addition and a topology. The commutative topological group X thus obtained is called the *character group* of the group G.

Let α and β be two elements of X. Their *sum*

$$\gamma = \alpha + \beta \tag{1}$$

is defined as follows. If $x \varepsilon G$, we let

$$\gamma(x) = \alpha(x) + \beta(x). \tag{2}$$

We then have

$$\gamma(x + y) = \alpha(x + y) + \beta(x + y) = \alpha(x) + \alpha(y) + \beta(x) + \beta(y) = \gamma(x) + \gamma(y).$$

Therefore γ is a homomorphism of the group G in the group K and hence $\gamma \varepsilon X$. The continuity of the mapping γ follows directly from the continuity of the mappings α and β. The *zero* of the group X is that homomorphism of the group G in the group K which maps every element of the group G into the zero of the group K. The homomorphism α' *inverse* to the homomorphism α, $\alpha' = -\alpha$, is determined by the relation $\alpha'(x) = -\alpha(x)$.

In order to introduce a topology into the group X we make use of Theorem 10, i.e., we define a complete system Σ^* of neighborhoods of zero of the group X. We find an arbitrary neighborhood V of the system Σ^* by starting with a neighborhood U of zero in the group K and an arbitrary compact set F of the group G. We then define the neighborhood V as the totality of all $\alpha \varepsilon X$ such that

$$(3) \qquad \alpha(F) \subset U.$$

It is not hard to verify that the system of neighborhoods Σ^* thus obtained satisfies all the conditions of Theorem 10, and therefore X becomes a topological group.

We make here the following preliminary remark.

B) There exists a neighborhood U of zero of the group K such that for any topological group G and character α of G, the relation

$$(4) \qquad \alpha(G) \subset U$$

implies that

$$(5) \qquad \alpha = 0.$$

We can define U as the set of all elements $a \varepsilon K$ which satisfy the inequalities $-\frac{1}{10} < a < \frac{1}{10}$ (see A)). Let us suppose that there exists an element $x \varepsilon G$ such that

$$(6) \qquad \alpha(x) \neq 0.$$

It can readily be seen that in that case there exists an integer n such that the element $n\alpha(x) = \alpha(nx)$ does not belong to U. Therefore relations (4) and (6) are contradictory so that (5) follows from (4).

THEOREM 31. *The character group X of the group G* (see Definition 34) *is always locally compact and satisfies the second axiom of countability. If the group G is discrete, then the group X is compact. If the group G is compact, the group X is discrete* (see §17, A)).

PROOF. We divide the proof into four parts.

a) X satisfies the second axiom of countability.

We shall show first of all that X contains a countable complete system of neighborhoods of zero.

Let

$$(7) \qquad U_1, \cdots, U_m, \cdots$$

be a countable complete system of neighborhoods of zero of the group K and let

$$(8) \qquad W_1, \cdots, W_n, \cdots$$

be a countable complete system of neighborhoods of the group G such that the closure $\overline{W}_n$ of every open set of the system (8) is compact. We denote by V_m^n a neighborhood of the system Σ^* (see Definition 34) defined by the neighborhood U_m and by the compact set $\overline{W}_1 \cup \overline{W}_2 \cup \cdots \cup \overline{W}_n$. The set of all neighborhoods V_m^n, $m = 1, 2, \cdots, n = 1, 2, \cdots$, is countable. We shall show that it forms a basis about zero (see §8, B')). Let V be a neighborhood of zero of the group X defined by a neighborhood U of zero of the group K and by a compact set F of the group G (see Definition 34). Then there exists a suffi-

ciently large number m such that $U_m \subset U$. Since the system (8) covers F, it follows from Theorem 7 that there exists a sufficiently large number n such that $F \subset W_1 \cup W_2 \cup \cdots \cup W_n$. It can readily be seen that $V_m^n \subset V$ (see (3)). Hence there exists a countable complete system of neighborhoods of zero of the group X.

In order to complete the proof that X satisfies the second axiom of countability it is now sufficient to show that X contains a countable everywhere dense set M (see §17, B)). We shall now construct this set M.

Let Γ be a countable complete system of neighborhoods in K, and Δ a countable complete system of neighborhoods in G such that if $B \varepsilon \Delta$, then $\overline{B}$ is compact. Furthermore, let

$$A_1, \cdots, A_r \tag{9}$$

be a finite sequence of elements of the system Γ, while

$$B_1, \cdots, B_r \tag{10}$$

is a finite sequence of elements of the system Δ. Starting with the sequences (9) and (10) we determine a set C of elements of the group X composed of all $\gamma \varepsilon X$ such that $\gamma(\overline{B}_k) \subset A_k$, $k = 1, \cdots, r$. There is only a countable number of sets of the type C. We select a single element from every non-null set of the type C, and denote the set thus obtained by M. The set M is countable. We shall show that it is everywhere dense in X.

Let α be an arbitrary element of X and V an arbitrary neighborhood of zero of the group X defined by a neighborhood U of zero of the group K and by a compact set F of G (see (3)). We shall show that there exists an element $\beta \varepsilon M$ such that $\beta - \alpha \varepsilon V$. This will show that M is everywhere dense in X.

For every $x \varepsilon F$ there exists a neighborhood $A_x \varepsilon \Gamma$ of the element $\alpha(x)$ such that

$$A_x - \alpha(x) \subset U \tag{11}$$

(see §2, A)). We denote further by $B_x \varepsilon \Delta$ such a neighborhood of the element $x \varepsilon F$ that

$$\alpha(\overline{B}_x) \subset A_x. \tag{12}$$

The system of all regions B_x, $x \varepsilon F$, covers F and therefore by Theorem 7 we can select a finite covering from this covering. Therefore there exists a finite system $x_1, \cdots, x_r$ of elements of F such that the system of open sets $B_{x_1}, \cdots, B_{x_r}$ covers F. The sequences

$$A_{x_1}, \cdots, A_{x_r} \tag{13}$$

and

$$B_{x_1}, \cdots, B_{x_r} \tag{14}$$

define, just as do the sequences (9) and (10), some set C' of the type C, where

$\alpha \varepsilon C'$. C' is not empty since $\alpha \varepsilon C'$, and therefore there exists an element β of the set C' belonging to M. We shall show that $\beta - \alpha = \delta \varepsilon V$. To do this it is sufficient to show that $\delta(F) \subset U$, i.e., if $y \varepsilon F$ we have $\beta(y) - \alpha(y) \varepsilon U$. But for every $y \varepsilon F$ there exists a number k such that $y \varepsilon B_{x_k}$ and therefore $\alpha(y) \varepsilon A_{x_k}$ (see (12)). On the other hand since $\beta \varepsilon C'$, it follows that $\beta(y) \varepsilon A_{x_k}$ and therefore by (11), $\beta(y) - \alpha(y) \varepsilon U$.

Hence, we have shown that X satisfies the second axiom of countability.

b) X is locally compact.

Let W be a neighborhood of zero in the group G whose closure $\overline{W}$ is compact. Let us denote by U the interval $-\frac{1}{10} < a < \frac{1}{10}$ in the group K, which is a neighborhood of zero in K. We define the neighborhood V of zero in the group X as the set of all elements α for which

$$\alpha(\overline{W}) \subset U \tag{15}$$

(see (3)). We shall show that V has a compact closure $\overline{V}$.

In order to show the compactness of $\overline{V}$, we show that every sequence

$$\alpha_1, \cdots, \alpha_n, \cdots \tag{16}$$

of elements of the set V has a limit element in X. We snow in particular that a convergent subsequence can be chosen from (16).

We shall consider the elements of U as numbers in the interval between $-\frac{1}{10}$ and $+\frac{1}{10}$ (see A)). Then every element $\alpha \varepsilon V$ defines a function $\alpha(x)$ on $\overline{W}$ which assumes numerical values not exceeding $\frac{1}{10}$ in absolute value. From this point of view the set V is a uniformly bounded family of *real-valued* continuous functions defined on $\overline{W}$. We shall show that this family is equicontinuous (see §24, D)).

Let ϵ be an arbitrary positive number, and $l > 10$ a sufficiently large positive number such that

$$\epsilon > \frac{1}{l} \cdot \tag{17}$$

We now denote by W' a neighborhood of zero of the group G such that if $z \varepsilon W'$, then

$$kz \varepsilon W, \qquad k = 1, \cdots, l. \tag{18}$$

Let us suppose that there exist two elements x and y of the set $\overline{W}$ and an element $\alpha \varepsilon V$ for which the following conditions are satisfied.

$$x - y = z \varepsilon W', \tag{19}$$

$$| \alpha(x) - \alpha(y) | = | \alpha(z) | > \epsilon. \tag{20}$$

We shall then arrive at a contradiction. To that end we consider the elements

$$\alpha(kz), \qquad k = 1, \cdots, l. \tag{21}$$

On the one hand it follows from relations (19), (18) and (15) that

$$(22) \qquad k\alpha(z) = \alpha(kz) \in U, \qquad k = 1, \cdots, l,$$

while on the other hand it follows from relations (20) and (17) that for some $k = k'$ we have $\frac{1}{10} < |k'\alpha(z)| < \frac{2}{10}$ and therefore the element $\alpha(k'z)$ cannot belong to U. This contradiction shows that for every positive ϵ there exists a neighborhood W' of zero of the group G such that if $x \in \overline{W}$, $y \in \overline{W}$, and $x - y \in W'$, then $|\alpha(x) - \alpha(y)| < \epsilon$ for every $\alpha \in V$. This means that the family V is equi-continuous.

Since the family V is equi-continuous and all the elements of the sequence (16) belong to V, we can select from that sequence a subsequence

$$(23) \qquad \beta_1, \cdots, \beta_n, \cdots$$

which converges uniformly in $\overline{W}$. Denote the limit of the subsequence by β. Then β is a continuous function on $\overline{W}$, whose values do not exceed $\frac{1}{10}$ in absolute value. We have in this way defined a continuous mapping β of the set $\overline{W}$ in $\overline{U}$. The uniform convergence of the sequence (23) can now be formulated as follows: for every neighborhood U'' of zero of the group K there exists a sufficiently large integer n', such that for $n > n'$ and $x \in \overline{W}$ we have

$$(24) \qquad \beta(x) - \beta_n(x) \in U''.$$

The set of all open sets of the form $g + W$, where $g \in G$, covers G, and therefore there exists a countable sequence

$$(25) \qquad g_1, \cdots, g_m, \cdots$$

of elements of the group G such that the totality of all open sets of the form

$$(26) \qquad g_m + W, \qquad m = 1, 2, \cdots,$$

covers G (see §12, H)). We now select a subsequence

$$(27) \qquad \gamma_1, \cdots, \gamma_n, \cdots$$

of the sequence (23), such that for every m there exists a limit

$$(28) \qquad \lim_{n\to\infty} \gamma_n(g_m) = \gamma(g_m).$$

Since the group K is compact, we can carry out this process of selection by means of the diagonal process (see Theorem 9)..

We shall now show that for every element $g \in G$ there exists the limit

$$(29) \qquad \lim_{n\to\infty} \gamma_n(g) = \gamma(g),$$

and that the mapping $\gamma(g)$ is a homomorphic mapping of the group G into the group K.

We note first of all that the sequence (27), being a subsequence of the sequence (23), converges uniformly on $\overline{W}$ (see (24)), and has for its limit the

mapping β. But, since the sequence of open sets (26) covers G every element $g \varepsilon G$ can be written in the form $g = g_m + x$, where $x \varepsilon W$. We have in this way

$$(30) \qquad \lim_{n\to\infty} \gamma_n(g) = \lim_{n\to\infty} \gamma_n(g_m) + \lim_{n\to\infty} \gamma_n(x) = \gamma(g_m) + \beta(x) = \gamma(g).$$

Furthermore, if g and h are two elements of G, then

$$\gamma(g + h) = \lim_{n\to\infty} \gamma_n(g + h) = \lim_{n\to\infty} \gamma_n(g) + \lim_{n\to\infty} \gamma_n(h) = \gamma(g) + \gamma(h).$$

Hence γ is a homomorphic mapping of the abstract group G in the abstract group K. It can readily be seen that the mapping γ is continuous (see §19, B)), and therefore is an element of the group X.

We shall now show that the sequence of homomorphisms (27) converges to the homomorphism γ in the sense of the topology established in X (see Definition 34).

Let $\gamma_n' = \gamma_n - \gamma$. It suffices to show that every neighborhood V' of zero of the group X contains all the elements of the sequence

$$(31) \qquad \gamma_1', \cdots, \gamma_n', \cdots$$

with the exception of only a finite number. Let us suppose that the neighborhood V' is defined by the compact set $F' \subset G$ and the neighborhood U' of zero of the group K (see Definition 34). Let U'' be a neighborhood of zero of the group K such that

$$(32) \qquad U'' + U'' \subset U'.$$

Since the system of open sets (26) covers the group G, we can select a finite subsystem

$$(33) \qquad g_m + W, \qquad m = 1, \cdots, r,$$

of open sets of the system (26) which covers the compact set F' (see Theorem 7). It follows from (28) that $\lim_{n\to\infty} \gamma_n'(g_m) = 0$. Therefore, there exists a sufficiently large n'' such that for $n > n''$ we have

$$(34) \qquad \gamma_n'(g_m) \varepsilon U'', \qquad m = 1, \cdots, r.$$

Furthermore, it follows from relation (24) that for $n > n'$ we have

$$(35) \qquad \gamma_n'(\overline{W}) \subset U''.$$

Relations (34), (35), and (32) for $n > n'$ and $n > n''$ imply $\gamma_n'(F') \subset U'$. Hence we have for $n > n'$ and $n > n''$ that $\gamma_n' \varepsilon V'$. Hence the sequence (31) converges to zero in the sense of the topology in the group X, and therefore the sequence (27) converges to γ.

It follows directly from the fact that every sequence of elements of the set V

has a limit point in X, that the set $\overline{V}$ is compact. Hence the local compactness of the group X is established.

c) If G is discrete, then X is compact.

In case G is discrete we can take for a neighborhood of zero in G (see b)) a set containing only the zero of the group G. Then the neighborhood V of the group X will be composed of all the elements of the group X (see (15)), and since we have already shown that $\overline{V}$ is compact (see b)), it follows that X is also compact.

d) If G is compact, then X is discrete.

For a compact group G we can take for a neighborhood W of zero the set G itself (see b)). Then condition (15) signifies, because of remark B), that V contains only the zero of the group X and therefore X is discrete.

Hence Theorem 31 is completely proved.

Theorem 31 shows, first of all, that by applying the operation of forming a character group to a locally compact commutative group which satisfies the second axiom of countability we obtain a group which satisfies the same conditions. In this way the set L of all locally compact commutative groups which satisfy the second axiom of countability forms a class closed with respect to the following operations: the formation of a subgroup, the formation of a factor group, the formation of the character group.

We denote by C the set of all commutative compact groups satisfying the second axiom of countability, and by D the set of all countable commutative discrete groups. Each of the classes C and D is closed with respect to the operations of forming subgroups and factor groups, but the operation of forming the character group gives a transition from one class into the other. In this way in the theory of characters, classes C and D are complements of one another. From this point of view it is more natural and economical to consider the whole class L at once so as not to separate cases, which would be inevitable in the consideration of classes C and D. It is worth noting, however, that the most important applications of the theory of characters are obtained for the classes C and D.

31. Fundamental Relations in the Theory of Characters

We shall formulate here, first of all, the fundamental Theorem 32 in the theory of characters. The proof of this theorem is rather complicated: it depends on the results of Peter and Weyl and on some delicate group-theory considerations. We shall develop all this gradually in the following sections. Here we shall also formulate the second fundamental Theorem 33 in the theory of characters, as a direct consequence of Theorem 32.

We have already remarked at the end of the preceding section that the class L of all locally compact commutative groups satisfying the second axiom of countability is closed with respect to the operations of forming subgroups, factor groups, and character groups. The present section is devoted to clearing up the connection between these three operations. It is true that since we give

no proof of Theorem 32 in this section, its most important consequences, namely Theorems 33 and 35 also remain for the moment without proof. Nevertheless it is desirable to have all these connections formulated in the same place.

A) Let X be the character group of the group G (see Definition 34). Then every element g of the group G represents in a natural way a definite character of the group X. In fact if $\alpha \in X$, then $g(\alpha)$ is defined by

$$g(\alpha) = \alpha(g), \tag{1}$$

where $\alpha(g)$ is defined because α is a character of the group G.

In order to prove that the mapping g of the group X in the group K defined by equation (1) is really a character of the group X, we consider two elements α and β of the group X. The sum of these elements $\gamma = \alpha + \beta$ is defined by equation (2) of §30, and we have

$$g(\gamma) = \gamma(g) = \alpha(g) + \beta(g) = g(\alpha) + g(\beta).$$

Hence g is a homomorphic mapping of the abstract group X in the abstract group K. In order to prove that g is continuous, it is sufficient to show that for every neighborhood U of zero of the group K there exists a neighborhood V of zero of the group X such that $g(V) \subset U$ (see §19, B)). We determine this neighborhood V of the group X from the neighborhood U of zero of the group K and from the compact set $F \subset G$ which contains only the point g. Then by Definition 34 the element $\alpha \in X$ belongs to the neighborhood V under the condition that $\alpha(g) \in U$, but this implies that $g(\alpha) \in U$, i.e., $g(V) \subset U$.

The meaning of remark A) is made clear by the following theorem.

THEOREM 32. *Let X be the character group of the group G* (see Definition 34). *By remark* A) *every element g of the group G represents a character of the group X. In this way G is a set of characters of the group X. The set G of characters, together with the topology and the addition defined in it, is the character group of the group X.*

The proof of this theorem will be given below (see §35). Here we shall only make some preliminary remarks leading up to the proof of Theorem 32.

B) Let X be the character group of the group G, and let G' be the character group of the group X. It follows from remark A) that every element $x \in G$ represents some definite character of the group X. To avoid misunderstanding we designate this character not merely by x but by $x' = \varphi(x)$. Then φ is a homomorphic mapping of the topological group G in the topological group G'.

We shall show first that φ is a homomorphic mapping of the abstract group G in the abstract group G'. Let x and y be two elements of G, and let $z = x + y$. Suppose further that $x' = \varphi(x)$, $y' = \varphi(y)$, and $z' = \varphi(z)$. If $\alpha \in X$, we have

$$z'(\alpha) = \alpha(z) = \alpha(x) + \alpha(y) = x'(\alpha) + y'(\alpha).$$

Hence $\varphi(x + y) = \varphi(x) + \varphi(y)$.

We shall now show that φ is a continuous mapping of the space G in the space G'. To do this it is sufficient to show that for every neighborhood V' of zero of the group G' there exists a neighborhood V of zero of the group G such that

(2) $$\varphi(V) \subset V'$$

(see §19, B)).

Let us suppose that the neighborhood V' is defined by the compact set $F' \subset X$ and by the neighborhood U' of zero of the group K (see Definition 34). Then property (2) of the neighborhood V can be formulated as follows,

(3) $$\text{if} \quad \alpha \varepsilon F' \quad \text{and} \quad x \varepsilon V, \quad \text{then} \quad \alpha(x) \varepsilon U'.$$

We now construct the neighborhood V which has this property. Since α is a continuous mapping, there exists a neighborhood V_α of zero of the group G such that

(4) $$\alpha(\overline{V}_\alpha) \subset U'$$

where $\overline{V}_\alpha$ is compact. Let U_α be a neighborhood of zero of the group K such that

(5) $$\alpha(\overline{V}_\alpha) + U_\alpha \subset U'.$$

We further define the neighborhood W_α of zero of the group X by the compact set $\overline{V}_\alpha \subset G$, and the neighborhood U_α of zero of the group K. Let us suppose

(6) $$W'_\alpha = \alpha + W_\alpha,$$

where W'_α is a neighborhood of the element α in the group X, having the following property: if $\beta \varepsilon W'_\alpha$ and $y \varepsilon V_\alpha$, then

(7) $$\beta(y) \varepsilon U'.$$

As α runs over the set F', the system of neighborhoods (6) covers this set. Let us select from this covering a finite covering $W'_{\alpha_1}, \cdots, W'_{\alpha_n}$ (see Theorem 7). The intersection of all the open sets V_{α_i}, $i = 1, \cdots, n$, we denote by V. It follows from (7) that if $\beta \varepsilon F'$ and $y \varepsilon V$, then $\beta(y) \varepsilon U'$. We have therefore found a neighborhood V of zero of the group G which possesses the desired property (3), and hence the mapping φ is continuous.

C) Let X be the character group of the group G. In order to prove Theorem 32 it is sufficient to prove the two following propositions.

a) For every element $x \varepsilon G$, distinct from zero, there exists an element $\alpha \varepsilon X$ such that $\alpha(x) \neq 0$.

b) Every character x' of the group X can be generated by means of some element x of the group G (see A)).

The proof of proposition C) follows directly from B). In fact if condition a) is satisfied then the mapping φ (see B)) has the identity for its kernel. Furthermore, if condition b) is satisfied, then the mapping φ is a mapping of the group G on the whole group G'. Under these two conditions the mapping φ

is an isomorphic mapping of the topological group G on the topological group G' (see Theorem 13 and §19, D)).

The value of Theorem 32 consists in the first place in that it allows us to consider every compact group G as the character group of a discrete group X (see Theorem 31). The consideration of the discrete group X can in turn be reduced essentially to the consideration of an abstract group X (see §17, A)) with a countable number of elements, for by Theorem 31, the discrete group X satisfies the second axiom of countability.

Theorem 32 establishes a complete symmetry between the groups G and X; each of these groups is the character group of the other. A further development of the duality of the groups G and X is given by Theorem 33. This theorem enables us to establish a one-to-one correspondence between the groups G and X. It is necessary, however, to precede Theorem 33 by the following definition.

DEFINITION 35. Let X be the character group of the group G (see Definition 34), and H a subgroup of the group G. Let us denote by (X, H) the set of all elements $\alpha \varepsilon X$ for which $\alpha(x) = 0$ for every $x \varepsilon H$. The set (X, H) is called the *annihilator* of the group H in the group X, and is a subgroup of the group X.

Let Φ be a subgroup of the group X, and let us denote by (G, Φ) the set of all elements $x \varepsilon G$ for which $\alpha(x) = 0$ for every $\alpha \varepsilon \Phi$. The set (G, Φ) is called the *annihilator* of the group Φ in the group G, and is a subgroup of the group G.

The fact that the sets (X, H) and (G, Φ) are subgroups of the groups X and G can be proved directly, and we shall therefore not stop to do so here.

THEOREM 33. *Let X be the character group of the group G* (see Definition 34) *and let H be a subgroup of the group G. Let $\Phi = (X, H)$ and $H' = (G, \Phi)$* (see Definition 35). *Then $H' = H$.*

The proof of Theorem 33 will be given later (see §35). Here we shall make only a preliminary remark:

D) Using the notation of Theorem 33 we have $H' \supset H$.

In fact if $x \varepsilon H$ and $\alpha \varepsilon \Phi$, then we have by Definition 35 that $\alpha(x) = 0$. On the other hand H' is defined as the totality of all the elements x for which $\alpha(x) = 0$. Hence $H' \supset H$.

THEOREM 34. *Let X be the character group of the group G* (see Definition 34), *and H a subgroup of the group G. Let $\Phi = (X, H)$* (see Definition 35). *Then the factor group $G^* = G/H$ has the group Φ for its character group. In greater detail: Every element $\alpha \varepsilon \Phi$ is a character of the group G^*: in fact if $x^* \varepsilon G^*$ then $\alpha(x^*)$ is defined by the equality*

$$\alpha(x^*) = \alpha(x) \tag{8}$$

where x is an arbitrary element of the coset x^*, and $\alpha(x^*)$ does not depend on the choice of x from this coset. Under these conditions the set Φ of characters together with its original topology and addition is the character group of the group G^*.

PROOF. First of all it is clear that equation (8) defines a mapping α of the group G^* in the group K. In fact let x and x' be two elements of the coset x^* and let $\alpha \varepsilon \Phi$. Then $\alpha(x) - \alpha(x') = 0$, since $\alpha(x - x') \varepsilon \alpha(H)$, and every homomorphism $\alpha \varepsilon \Phi$ maps the whole group H into zero. Hence $\alpha(x) = \alpha(x')$.

We shall show now that the mapping α of the group G^* in the group K is a homomorphic mapping. If x^* and y^* are two elements of the group G^* and $x \varepsilon x^*$, $y \varepsilon y^*$, then the sum $z^* = x^* + y^*$ is defined as the coset containing the element $z = x + y$. We obtain in this way

$$\alpha(z^*) = \alpha(z) = \alpha(x) + \alpha(y) = \alpha(x^*) + \alpha(y^*).$$

Hence α is a homomorphic mapping of the abstract group G^* in the abstract group K. Let us show that α is a continuous mapping of the group G^* in the group K. Let U be a neighborhood of zero of the group K. Then there exists a neighborhood V of zero of the group G such that $\alpha(V) \subset U$. Let us denote by V^* the totality of all cosets of the form $u + H$, where $v \varepsilon V$. Then V^* is a neighborhood of zero of the group G^*. Obviously, $\alpha(V^*) \subset U$, since $\alpha(H) = (0)$. Hence the mapping α of the group G^* is continuous, and therefore is a homomorphic mapping of the topological group G^* in the topological group K.

We denote by Φ' the character group of the group G^*. From what we have already shown every element $\alpha \varepsilon \Phi$ is a character of the group G^*. We shall denote this character not by α, but by

$$\alpha' = \psi(\alpha) \tag{9}$$

and show that ψ is an isomorphic mapping of the group Φ on the group Φ'.

We denote by f the natural homomorphic mapping of the group G on the group G^* (see §19, C)). Then equation (9) is equivalent to the relation

$$\alpha(x) = \alpha'(f(x)), \tag{10}$$

where x is an arbitrary element of G. If α' is an arbitrary element of Φ', then relation (10) defines an element $\alpha \varepsilon \Phi$ such that $\psi(\alpha) = \alpha'$. Hence the mapping ψ is a mapping on the whole group Φ'. Furthermore, relation (10) enables us to define for every element α' a corresponding element α, since the mapping ψ is one-to-one, and we can consider its inverse ψ^{-1}. We shall show that the mapping ψ^{-1} is isomorphic. Let α' and β' be two arbitrary elements of Φ' and let $\gamma' = \alpha' + \beta'$. Let also

$$\alpha = \psi^{-1}(\alpha'), \qquad \beta = \psi^{-1}(\beta'), \qquad \gamma = \psi^{-1}(\gamma').$$

Then we have

$$\gamma(x) = \gamma'(f(x)) = \alpha'(f(x)) + \beta'(f(x)) = \alpha(x) + \beta(x).$$

Hence

$$\psi^{-1}(\alpha' + \beta') = \psi^{-1}(\alpha') + \psi^{-1}(\beta')$$

and therefore the mapping ψ^{-1} is an isomorphic mapping of the abstract group

Φ' on the abstract group Φ. It remains to be shown that ψ^{-1} is continuous. Let V be an arbitrary neighborhood of zero of the group X. Suppose V is defined by the compact set $F \subset G$ and by a neighborhood U of zero of the group K (see Definition 34). Suppose $f(F) = F^*$ and let us define the neighborhood V' of zero of the group Φ' by the compact set $F^* \subset G^*$ (see Theorem 8), and by the neighborhood U. Obviously in this case

$$(11) \qquad \psi^{-1}(V') \subset V,$$

since if $\alpha' \varepsilon V'$, then $\alpha(F) = \alpha'(f(F)) = \alpha'(F^*) \subset U$. Relation (11) shows that the mapping ψ^{-1} is continuous (see §19, B)). Hence ψ is an isomorphic mapping (see Theorem 13 and §19, D)).

Hence Theorem 34 is proved.

E) Let X be the character group of the group G and H a subgroup of the group G. Let $\Phi = (X, H)$. If Theorem 32 is true for the factor group $G^* = G/H$ and the group Φ (see Theorem 34), then Theorem 33 is also true, i.e. $H' = H$, where $H' = (G, \Phi)$.

By Theorem 34 the group G^* has for its character group the group Φ. Since Theorem 32 is true by assumption for these groups, it follows that G^* is in turn the character group of the group Φ. Let us suppose that there exists an element x of H' which is not in H. We denote by x^* that element of the group G^* which, considered as a coset, contains the element x. Since x does not belong to H, it follows that $x^* \neq 0$. By its construction, H' is composed of all the elements of G which are mapped into zero by all the characters of Φ. Hence the element x^* is mapped into zero by any character of Φ, i.e., $\alpha(x^*) = 0$ for every $\alpha \varepsilon \Phi$. On the other hand, x^* is a non-zero character of the group Φ, since $x^* \neq 0$, and therefore there exists an element $\beta \varepsilon \Phi$ such that $x^*(\beta) \neq 0$. But $x^*(\beta) = \beta(x^*)$ and we have arrived at a contradiction. Hence $H' \subset H$; but by D) we have $H' \supset H$, and therefore $H' = H$.

THEOREM 35. *Let G be a topological group, H a subgroup of G, y an element of G which does not belong to H, and β^* a character of the group H. Then there exists a character α of the group G such that $\alpha(y) \neq 0$ and $\alpha(x) = \beta^*(x)$ for every $x \varepsilon H$. The character α becomes in this way an extension of the character β^*.*

Theorem 35, just as Theorem 33, is a direct consequence of Theorem 32. We shall indicate here a way of reducing Theorem 35 to Theorem 32.

F) If Theorem 32 is true, then Theorem 35 is also true.

Let X be the character group of the group G. Let $\Phi = (X, H)$ and $X^* = X/\Phi$. Since Theorem 32 is true by assumption, it follows from E) that $H = (G, \Phi)$. From Theorem 32, G is the character group of the group X and therefore we can assert by Theorem 34 that H is the character group of the group X^* and, conversely, X^* is the character group of the group H.

Since β^* is a character of the group H, $\beta^* \varepsilon X^*$. We denote by β an element of the coset β^*. Then $\beta(x) = \beta^*(x)$ for $x \varepsilon H$. If now $\beta(y) \neq 0$, then our proposition is proved. In case $\beta(y) = 0$, some further considerations are

necessary. Let us consider this case. Since y is not in H, there exists an element $\gamma \varepsilon \Phi$ such that $\gamma(y) \neq 0$. Suppose $\alpha = \beta + \gamma$. Then $\alpha(y) = \beta(y) + \gamma(y) = \gamma(y) \neq 0$. At the same time $\alpha(x) = \beta(x)$ for $x \varepsilon H$, since $\gamma(x) = 0$ as $\gamma \varepsilon \Phi$.

32. Simple Examples and Preliminary Considerations

We shall consider here the character groups of the simplest groups. We shall establish the truth of Theorem 32 for these groups. This will not only serve as a concrete example, but will also form the foundation of the proof of Theorem 32 in the general case.

First of all we establish some properties of the group K (see §30, A)).

A) Every subgroup N of the group K either coincides with K, or else is of a finite order r, $r = 1, 2, \cdots$. In the latter case, all the elements of the group N can be expressed in the form

$$p/r, \qquad p = 0, 1, \cdots, r - 1 \tag{1}$$

(see §30, A)). Hence N is a cyclic group with the generator $1/r$. If N is finite, it can be characterized as the group composed of all the elements of the set K of finite order whose orders divide the number r.

Suppose that the group N is infinite. Then there exists an element in K which is a limit element for the subset N, and hence N contains two elements a and b arbitrarily close to each other. The difference $c = a - b$ is arbitrarily close to zero, and its multiples nc, $n = 1, 2, \cdots$, which belong to N, fill up the group K arbitrarily densely. Since the set N is closed in K, it follows that $N = K$.

Let us now consider the case of a finite group N of order r. If $a \varepsilon N$, then $ra = 0$, which means that the element a can be written numerically as p'/r. It is obvious that every element of the form p'/r can be written in the form p/r, where $0 \leqq p < r$. The totality of all the elements p/r, $p = 0, 1, \cdots, r - 1$, forms a group of order r. We can conclude from this that N is composed of all the elements of the form (1), since the elements which are not of that form cannot belong to N, and there are just r elements of the form (1).

B) There are only two automorphisms of the group K, the identical automorphism, $\alpha(x) = x$, and another automorphism β for which $\beta(x) = -x$.

Let γ be an arbitrary automorphism of the group K. The only element of order 2 in the group K is $1/2$ (see A)); therefore $\gamma(1/2) = 1/2$. K contains only two elements of order 4, namely $1/4$, and $-1/4$. There are therefore two possible cases, $\gamma(1/4) = 1/4$ and $\gamma(1/4) = -1/4$. These two cases are realized by the automorphisms α and β. We shall show that no other automorphisms exist. Let us consider the case in which $\gamma(1/4) = 1/4$. The element $1/8$ can go over under the automorphism γ only into one of the elements $1/8$, $3/8$, $5/8$, or $7/8$, but since the automorphism γ is a continuous mapping it preserves the cyclic order on K, and knowing that

$$\gamma(0) = 0, \qquad \gamma(1/4) = 1/4, \qquad \gamma(1/2) = 1/2, \qquad \gamma(3/4) = 3/4,$$

we conclude that $\gamma(1/8) = 1/8$. Continuing in this way we conclude that $\gamma(1/2^n) = 1/2^n$. Multiplying the last equation by a positive integer $m < 2^n$, we get $\gamma(m/2^n) = m/2^n$. It follows from the continuity of the automorphism γ and from the last relation that γ is the identical automorphism. Similarly, the case in which $\gamma(1/4) = -1/4$ leads to $\gamma = \beta$.

C) Every homomorphism α of the group K into itself can be expressed in the form $\alpha(x) = mx$, where m is an integer which characterizes the homomorphism α, $\alpha = \alpha_m$. If α_m and α_n are two homomorphisms of the group K into K, i.e., two characters, then

$$\alpha_m + \alpha_n = \alpha_{m+n}.$$

Let N be the kernel of the homomorphism α. From remark A), N either coincides with K, or else is finite and is characterized by a positive number r. If $N = K$, then $\alpha(x) = 0 \cdot x$. Suppose that N is finite. Then the factor group $K' = K/N$ can readily be seen to be isomorphic with the group K. The question now arises as to how to establish an isomorphic mapping of the group K' on the group K, since it is not possible to have an isomorphic mapping of the group K' on a subgroup of the group K. It follows from B) that there exist only two isomorphic mappings of the group K' on the group K, and they correspond to the two distinct cases $\alpha(x) = rx$ and $\alpha(x) = -rx$. Hence C) is proved.

D) Let G be an infinite cyclic group, i.e., a group isomorphic with the additive group of integers. Then the character α of the group G can be given by the relations $\alpha(ng) = na$, where g is a generator of the group G and a an arbitrary element of the group K. The element a determines the character $\alpha = \alpha_a$. The sum of two characters is defined by the formula, $\alpha_a + \alpha_b = \alpha_{a+b}$.

Proposition D) is obvious.

E) Let G be a finite cyclic group of order r. Then every character α of the group G is defined by the relation $\alpha(ng) = np/r$, where g is a generator of the group G and p/r an element of the group K, written in fractional form. The character α is defined by the element p/r, and we write $\alpha = \alpha_{p/r}$. The sum of two characters is defined by the formula $\alpha_{p/r} + \alpha_{q/r} = \alpha_{(p+q)/r}$.

Proposition E) follows directly from remark A).

F) Let G be a discrete infinite cyclic group, and let X be the character group of the group G. Then X is isomorphic with the group K and Theorem 32 is true for the pair G, X.

This follows directly from remarks D) and C).

G) Let G be a finite cyclic group and X its character group. Then X is isomorphic with G and Theorem 32 is true for the pair G, X.

This proposition follows directly from remark E).

H) Let G be the topological additive group of all real numbers. Then every character α of the group G can be expressed in the form $\alpha(x) = dx$, where x is an arbitrary element of the group G, d is a real number defining the character α, $\alpha = \alpha_d$, and where the right side is defined up to an additive in-

teger. The sum of two characters of the group G is defined by the formula $\alpha_c + \alpha_d = \alpha_{c+d}$.

Let N be the kernel of the homomorphism α. If $N = G$ we have the case $\alpha(x) = 0 \cdot x$. If N does not coincide with G, then N contains a least positive number t, and N is an infinite cyclic group with the generator t. Then the group $K' = G/N$ is isomorphic with the group K, and we are to find the isomorphism which will map the group K' on K. By B) there are then only two possible cases: $\alpha(x) = x/t$ and $\alpha(x) = -x/t$. Hence H) is proved.

I) Let G be the topological additive group of all real numbers, and let X be the character group of the group G. Then X is isomorphic with G and Theorem 32 is true for the pair G, X.

This follows directly from remark H).

The following proposition enables us to construct character groups and to prove Theorem 32 for a wider class of groups.

Theorem 36. *Let*

$$G_1, \cdots, G_r \tag{2}$$

be a finite system of topological groups. Let us denote by X_i the character group of the group G_i. Furthermore, let G be the direct sum of the groups of the system (2), *and X the direct sum of*

$$X_1, \cdots, X_r. \tag{3}$$

Then X is the character group of the group G. In greater detail, if $x = (x_1, \cdots, x_r)$ is an element of the group G and $\alpha = (\alpha_1, \cdots, \alpha_r)$ an element of the group X, then the character α of the group G is defined by the relation

$$\alpha(x) = \alpha_1(x_1) + \cdots + \alpha_r(x_r). \tag{4}$$

Furthermore, if Theorem 32 *is true for the groups of the system* (2), *then it is also true for the group G.*

Proof. It is obvious, first of all, that relation (4) actually gives a character of the group G. Let α' be an arbitrary element of the group G. Since the groups of the system (2) can be regarded as subgroups of the group G, the character α' is defined also for the group G_i, i.e., to the character α' corresponds a definite character α'_i of the group G_i. It is not hard to verify that $\alpha' = (\alpha'_i, \cdots, \alpha'_r)$. Hence the set X contains all the characters of the group G. In the same way, it is not hard to verify that X is the character group of the group G.

Now let x' be an arbitrary element of the group X. Just as above, to x' corresponds a definite character x'_i of the group X_i. Since Theorem 32 is true by assumption for the pair G_i, X_i, it follows that $x'_i \in G_i$. Hence there exists an element $(x'_i, \cdots, x'_r) = x''$ in G. It can easily be verified that $x' = x'' \in G$.

Hence Theorem 36 is completely established.

J) If the discrete group G has a finite system of generators, (see §6, B)), and

if X is the character group of the group G, then Theorem 32 is true for the pair G, X. We shall call the group X a *generalized toroidal* group.

This follows directly from proposition F) of §6 and Theorem 36 together with remarks G) and F).

K) Let G be a discrete group having a finite system of linearly independent generators (see §6, A), B)) and X its character group. Then X can be decomposed into a direct sum of a finite number of groups isomorphic with the group K, and we shall therefore call X a *toroidal group*. The generalized toroidal group (see J)) can be decomposed into the direct sum of a toroidal group and a finite group.

The proof of this proposition follows directly from F) of §6, and Theorem 36 together with remarks G) and F).

L) Let G be the additive topological vector group, and X its character group. Then X is isomorphic with G, and Theorem 32 is true for the pair G, X.

Since the vector group G can be decomposed into the direct sum of groups isomorphic with the group of real numbers, proposition L) follows directly from Theorem 36 and remark I).

We shall now make two preliminary remarks of a general character.

LEMMA. *Let G be a topological group, and H a subgroup of G such that the factor group G/H is discrete. Let β be a character of the group H and g an element of G not belonging to the subgroup H. Then the character β can be extended to some character α of the whole group G in such a way that $\alpha(g) \neq 0$. In other words our lemma asserts the truth of Theorem* 35 *in case the factor group G/H is discrete.*

PROOF. Since the factor group G/H is discrete, there exist only a countable number of cosets of the subgroup H in the group G. Let us select a single element from each coset, and denote the elements selected by

$$g_1, \cdots, g_n, \cdots, \tag{5}$$

where we let $g_1 = g$. We denote by H_n the minimal subgroup of the group G which contains the subgroup H and the finite system of elements $g_1, \cdots, g_n$, and by H_0 the subgroup H itself. We now construct by induction the sequence of characters

$$\beta_0 = \beta, \beta_1, \cdots, \beta_n, \cdots, \tag{6}$$

where β_{n+1} is a character of the group H_{n+1} and is the extension of the character β_n. As soon as the construction of the sequence (6) is effected, the lemma is proved, the character α being defined by setting $\alpha = \beta_n$ on the group H_n. Since every element of the group G is in one of the groups H_n, α is defined over the whole group G. The homomorphism α coincides with β on H, and since H contains a neighborhood of zero of the group G, the continuity of α follows from the continuity of β (see §19, B)). Hence it remains only to verify that $\alpha(g) \neq 0$.

Let us suppose that the homomorphism β_n has already been constructed, and

let us construct the homomorphism β_{n+1}. In doing this we have to separate three cases:

a) If the element $g_{n+1} \varepsilon H_n$, then $H_{n+1} = H_n$, and we have

$$\beta_{n+1} = \beta_n.$$

b) If no multiple of the element g_{n+1} belongs to the subgroup H_n, then every element $x \varepsilon H_{n+1}$ can be written uniquely in the form $x = y + mg_{n+1}$ where $y \varepsilon H_n$ and m is an integer. In this case we shall suppose that

$$\beta_{n+1}(x) = \beta_n(y) + ma,$$

where a is an element of the group K. In case $n = 0$ we shall suppose that $a \neq 0$ in order that $\beta_1(g)$ should not map into zero. If $x = y + mg_{n+1}$ and $x' = y' + m'g_{n+1}$ are two elements of the group H_{n+1}, then we have

$$\begin{aligned}\beta_{n+1}(x + x') &= \beta_n(y + y') + (m + m')a = \beta_n(y) + ma + \beta_n(y') + m'a \\ &= \beta_{n+1}(x) + \beta_{n+1}(x').\end{aligned}$$

Hence β_{n+1} is a character of the group H_{n+1}.

c) Let $r > 1$ be an integer such that $rg_{n+1} \varepsilon H_n$, and suppose r is the least number satisfying this condition. Then every element x of the group H_{n+1} can be written uniquely in the form $x = y + mg_{n+1}$ where $y \varepsilon H_n$, and m is a non-negative number less than r. Let a be an element of K such that $ra = \beta_n(rg_{n+1})$. There always exist one or more elements a satisfying this condition. Therefore, if $n = 0$, we can suppose that $a \neq 0$. The character β_{n+1} is now defined by the relation

$$\beta_{n+1}(x) = \beta_n(y) + ma.$$

Let $x = y + mg_{n+1}$ and $x' = y' + m'g_{n+1}$ be two elements of the group H_{n+1}. Let us denote by j a number which is equal to zero if $m + m' < r$, and which is equal to one if $m + m' \geqq r$, so that $0 \leqq m + m' - jr < r$. We then have

$$\begin{aligned}\beta_{n+1}(x + x') &= \beta_n(y + y' + jrg_{n+1}) + (m + m' - jr)g \\ &= \beta_n(y) + \beta_n(y') + j\beta_n(rg_{n+1}) + ma + m'a - jra \\ &= \beta_n(y) + ma + \beta_n(y') + m'a = \beta_{n+1}(x) + \beta_{n+1}(x').\end{aligned}$$

Hence β_{n+1} is a character of the group H_{n+1}, and the lemma is proved.

As a consequence of this lemma we have the following proposition:

M) Let X be the character group of the group G and H a subgroup of the group G such that G/H is discrete. Let $\Phi = (X, H)$ (see Definition 35). Then H has for its character group the group $X^* = X/\Phi$. This can be stated in greater detail as follows; If α and α' are two elements of the group X belonging to the same coset of the subgroup Φ, then the characters α and α' coincide on H. In this way every element of the group X^* can be regarded as a character of the group H, and X^*, taken as the set of all these characters to-

gether with its original topology and addition, is the character group of the group H.

Let us denote by $X^{*\prime}$ the character group of the group H. Every character α of the group G defines on the subgroup H some character $\psi(\alpha)$. It can be checked in a trivial way that the mapping ψ is a homomorphic mapping of the abstract group X on the abstract group $X^{*\prime}$. It is also not hard to see that the mapping ψ is continuous. Roughly speaking this can be expressed by saying that two homomorphisms which are neighboring on G will also be neighboring on H. It follows from the fact that every character of the group H can be extended into a character of G (see the Lemma) that the mapping ψ is a mapping on the whole group $X^{*\prime}$. Furthermore, the character $\alpha \varepsilon X$ maps into zero on the group H if and only if $\alpha \varepsilon \Phi$. Hence the kernel of the homomorphism ψ is Φ. By Theorems 13 and 12 the group $X^{*\prime}$ is isomorphic with X/Φ and hence proposition M) is proved.

Example 47. Let G be a compact commutative topological group. If $g(x)$ is a representation of the first degree of the group G (see Definition 32), we shall consider $g(x)$ not as a matrix of order one, but simply as a number. This number, as can easily be seen, has absolute value unity. Let $\alpha(x) = \log (g(x))/2\pi i$. Then $\alpha(x)$ is a real number, defined up to an additive integer, and hence $\alpha(x)$ can be treated as an element of the group K (see §30, A)). It is not hard to verify that $\alpha(x)$ is a character of the group G (see Definition 34). Conversely if $\beta(x)$ is a character of the group G then $h(x) = e^{2\pi i\beta(x)}$ is a representation of the first degree of the group G

Let $G = K$. Then $g_n(x) = e^{2\pi inx}$ is a representation of the group $G = K$ (see Example 44), and the corresponding character $\alpha_n(x) = \log (g_n(x))/2\pi i = nx$. The set $\alpha_n(x)$, $n = 0, \pm 1, \pm 2, \cdots$, contains all the characters of the group K (see C)), and therefore the corresponding set $g_n(x)$, $n = 0, \pm 1, \pm 2, \cdots$, gives a complete system of irreducible representations of the group K. Hence by Theorem 27 the system of functions $g_n(x)$, $n = 0, \pm 1, \pm 2, \cdots$, is a complete orthogonal system. Conversely, proposition C) can be made to follow from a theorem in analysis concerning the completeness of this system of functions.

33. Compact and Discrete Groups

We shall prove here for compact and discrete groups the propositions which we have formulated in §31. We shall be concerned primarily with Theorem 32, since Theorems 33 and 35 follow as corollaries. We shall also give Theorem 38, which has no analogue for general locally compact groups. By way of applications of the results of this section we shall give Examples 48 and 49, which, however, are not devoid of general value.

A) Let G be a discrete group and X its character group. Then Theorem 32 is true for the pair G, X. (We should recall here that the group X is compact by Theorem 31.)

To prove this, we make use of remark C) of §31. Let $g_1, \cdots, g_n, \cdots$ be

the totality of all the elements of the group G. Let us denote by H_n the minimal subgroup of the group G which contains the elements

(1) $$g_1, \cdots, g_n.$$

Then the group H_n has a finite system of generators, namely the system (1). Furthermore, the sequence

(2) $$H_1, \cdots, H_n, \cdots$$

is non-decreasing, and it exhausts the whole group G, i.e., an arbitrary element $x \in G$ is contained in one of the members of the sequence (2). Let now $\Phi_n = (X, H_n)$, (see Definition 35). Since the sequence (2) is non-decreasing it follows that the sequence

(3) $$\Phi_1, \cdots, \Phi_n, \cdots$$

is non-increasing, i.e., $\Phi_{n+1} \subset \Phi_n$, $n = 1, 2, \cdots$. Since, moreover, the sequence (2) comprises the whole group G, it follows that the intersection of all the elements of the sequence (3) contains only the zero of the group X. We can conclude from this that for every neighborhood V of zero of the group X, a sufficiently large number m can be found such that

(4) $$\Phi_m \subset V$$

(see §13, C)).

We shall show that condition b) of remark C) of §31 is satisfied. Let x be a character of the group X, and U the neighborhood of zero of the group K considered in remark B) of §30. Let us denote by V a neighborhood of zero of the group X such that $x(V) \subset U$. It follows from (4) that $x(\Phi_m) \subset U$, but by remark B) of §30 this means that $x(\Phi_m) = 0$. Hence the character x of the group X can be looked upon as a character of the factor group $X^* = X/\Phi_m$ (see Theorem 34). By remark M) of §32 the group H_m has for its character group the group X^*, but since the group H_m admits a finite system of generators, it follows from remark J) of §32 that H_m is in turn the character group of the group X^*. Hence the character x of the group X^* is contained among the elements of the group H_m, or $x \in H_m$, which means that x, being a character of the group X, belongs to the group G.

We shall now show that condition a) of remark C) of §31 also holds here. Let g be an element of the group G, distinct from zero. Let us denote by β the null character of the null subgroup of the group G. The conditions of the lemma of §32 are satisfied here, and hence there exists a character α of the group G such that $\alpha(g) \neq 0$.

In this way, A) follows from remark C) of §31.

B) Theorem 33 is true for a discrete group G.

This statement is a direct consequence of remark E) of §31 and proposition A).

In order to prove Theorem 32 for a compact group G, we formulate in terms of the notation of the present chapter the single result of the theory of representations which we shall need in this chapter.

C) If G is a compact group, and a one of its elements, distinct from zero, then there exists a character α of the group G such that $\alpha(a) \neq 0$.

By Theorem 28 there exists an irreducible representation g of the group G such that $g(a)$ is not a unit matrix. By Theorem 26 the irreducible representation g is of the first degree, and hence $g(x)$ is a unitary matrix of the first order. We shall treat $g(x)$ simply as a complex number of absolute value unity. Let $\alpha(x) = \log (g(x))/2\pi i$. Then $\alpha(x)$ is an element of the group K, and since g is a representation, α is a character of the group G. Since $g(a) \neq 1$, $\alpha(a) \neq 0$.

D) If G is a compact group and X its character group, then Theorem 32 is true for the pair G, X. (We recall here that X is discrete by Theorem 31.)

To prove this we shall make use of remark B) of §31. Let G' be the character group of the group X. By Theorem 31, the group G' is compact. Furthermore, by remark B) of §31, there exists a natural homomorphic mapping φ of the group G in the group G'. We shall show that this mapping is isomorphic By remark C) there exists for every element $a \in G$, distinct from zero, a character $\alpha \in X$ such that $\alpha(a) \neq 0$. But this implies that the character $\varphi(a)$ of the group X does not map the element α into zero, and therefore $\varphi(a) \neq 0$. Hence the mapping φ is an isomorphic mapping of the group G on the subgroup $\varphi(G)$ of the group G', since the set $\varphi(G)$, being compact, is closed in G'. We shall simply say that by means of the isomorphism φ the group G is imbedded in the group G', or $\varphi(G) = G$.

We shall now show that $G = G'$. Suppose the contrary is true. Then there exists an element b belonging to G', but not to G. We denote the factor group G'/G by G^*, and the coset containing b by b^* Since b is not in G, $b^* \neq 0$. Hence by C) there exists a character α of the group G^* such that $\alpha(b^*) \neq 0$. A character α of the factor group G^* can be looked upon as a character of the group G' (see Theorem 34) with $\alpha(G) = 0$. G' is the character group of the group X, but by A) the group X is in turn the character group of the group G'. Hence $\alpha \in X$. But the character α of the group G' maps the whole group G into zero, while the group X was originally defined as the character group of the group G. Therefore α is the null element of the group X, but then $\alpha(b^*) = 0$. Hence we have arrived at a contradiction, and $G' = G$, which proves D).

E) Theorem 33 is true for a compact group G.

This follows directly from remark E) of §31 and from D).

Theorem 37. *If G is compact or discrete all propositions of* §31 *hold.*

Proof. Theorems 32 and 33 are proved in this case in A), B), D), and E). Theorem 35 is also true since in case the group G is compact or discrete all the groups encountered in the proof of this theorem are also compact or discrete (see §31, F)).

We could conclude here the consideration of compact and discrete groups were it not for an important proposition which unfortunately has no analogue in the general case.

Definition 36. Let G be a discrete group, and X a compact group. We shall say that the groups G and X form a *pair* if there exists a law of multiplication of the elements of the group G by the elements of the group X, i.e., to every pair of elements $x \varepsilon G$ and $\xi \varepsilon X$ there corresponds an element $a \varepsilon K$, called the *product* of the elements x and ξ, $x\xi = \xi x = a \varepsilon K$. Moreover, two distributive laws, and a condition of continuity of the product have to be satisfied. The distributive laws have the following form; $(x + x')\xi = x\xi + x'\xi$, $x(\xi + \xi') = x\xi + x\xi'$. The condition of continuity is as follows: if $\lim_{n \to \infty} \xi_n = \xi$, where $\xi_n \varepsilon X$, $n = 1, 2, \cdots$, and if $\xi \varepsilon X$, then $\lim_{n \to \infty} x\xi_n = x\xi$, where x is an arbitrary element of G.

Let H be a subgroup of the group G. We shall call the set of all elements ξ of the group X for which $x\xi = 0$ for every $x \varepsilon H$ the *annihilator* (X, H). In the same way we introduce the annihilator (G, Φ), where Φ is a subgroup of the group X. It is not hard to show that the annihilators are subgroups.

If the following conditions are satisfied for the pair G, X

$$(G, X) = \{0\} \qquad (X, G) = \{0\}$$

then this pair is called *orthogonal.*

F) If G and X form a pair, then every element $x \varepsilon G$ represents naturally a character of the group X. In order to determine the character x it is sufficient to let $x(\xi) = x\xi$, where the right side is defined since G and X form a pair (see Definition 36). In the same way every element ξ of the group X is a character of the group G.

The following theorem, which is very convenient for applications, is a direct consequence of the theory of characters:

Theorem 38. *If G and X form an orthogonal pair, then each of these groups is the character group of the other.*

Proof. Let G' be the character group of the group X. Since X is compact, it follows that G' is discrete (see Theorem 31). By F) every element $x \varepsilon G$ is a character of the group X. We denote this character by $x' = \varphi(x)$. Using the same considerations which were used to prove B) of §31, it is easy to show that the mapping φ of the group G in the group G' is homomorphic. The proof is considerably simplified here by the fact that G and G' are discrete, and hence all topological considerations may be omitted. Furthermore, it can readily be seen that the mapping φ is isomorphic. In fact, let a be an arbitrary element of the group G distinct from zero. Since the groups G and X are orthogonal there exists an element $\alpha \varepsilon X$ such that $a\alpha \neq 0$, and this implies that the character $\varphi(a)$ is not null. Hence φ is an isomorphic mapping of the group G on a subgroup G'' of the group G'. Because of the orthogonality we have $(X, G'') = \{0\}$. But since G' is the character group of the group X it follows

from Theorem 32 and 33 (see Theorem 37) that $G'' = (G'\{0\}) = G'$. Hence $G'' = G'$, and the group G is the character group of the group X. We can conclude from this with the help of Theorem 32 (see Theorem 37) that the group X is the character group of the group G.

Hence Theorem 38 is proved.

The proof of the corresponding theorem in the general case of locally compact groups does not go through because it is not possible to assert that G'' is a subgroup of the group G', since the subset G'' may not be closed in G'. Example 50 (see below) shows that Theorem 38 is actually not true in the general case.

In Examples 48 and 49 given below we shall make clear the connection between the topological properties of the character group X of a discrete group G and the algebraic properties of the group G itself.

EXAMPLE 48. Let G be a discrete group and X its character group. We shall show that X is connected if and only if the group G has no elements of finite order.

Suppose that G contains an element a of finite order $r > 1$. We denote by H the cyclic subgroup of the group G having the generator a. The group H is finite and is of order r. Let $\Phi = (X, H)$. Then by Theorem 33 (see Theorem 37) we have $H = (G, \Phi)$. Furthermore, by Theorem 32 (see Theorem 37) the group G is the character group of the group X. We can conclude from this and from Theorem 34 that the group X/Φ has the group H for its character group. But then the group X/Φ is the character group of the group H. It follows from remark G) of §32 that the group X/Φ is of finite order r. Hence the group X can be mapped continuously on the finite set X/Φ, which contains more than one element. But this means that X is not connected.

Let us now suppose that X is not connected, and let X' be the component of zero of the group X (see §22, A)). Then the factor group $X/X' = X^*$ is a 0-dimensional group (see §22, C)). Let us select in X^* a small open subgroup Φ^* (see Theorem 17). Then X^*/Φ^* is a finite group (see §22, E)). We denote by Φ the inverse image of the group Φ^* in the group X under the natural homomorphic mapping. Then X/Φ is also finite and contains more than one element. Let $H = (G, \Phi)$. Then H is the character group of the group X/Φ, and hence H is a finite subgroup of the group G, i.e., G contains elements of finite order.

EXAMPLE 49. Let G be a discrete group and X its character group. We shall show that the dimension of the group X is equal to the rank of the group G (see §6, A)).

Suppose that the rank of the group G is finite and is equal to r. We shall show that in this case the dimension of the group X does not exceed r. Let H_n, $n = 1, 2, \cdots$, be an increasing sequence of subgroups of the group G which comprises the whole group G, such that each group of the sequence admits a finite system of generators. Let $\Phi_n = (X, H_n)$; then the group $X_n^* = X/\Phi_n$ is the character group of the group H_n. Since H_n admits a finite system of

generators, it follows that X_n^* is a generalized toroidal group (see §32, J)), and it can be seen directly that the dimension of the group X_n^* is equal to the rank of the group H_n, but, obviously, the rank of the group H_n does not exceed r. Since the group Φ_n is by construction arbitrarily small, it can easily be proved (see §44, F)) that the dimension of the group X itself does not exceed the number r.

In order to give a lower bound for the dimension of the group X we consider the component of zero X' of the group X. Let $H = (G, X')$. From considerations similar to those of Example 48 it follows readily that H is composed of all the elements of the group G having a finite order. Therefore the group $G^* = G/H$ has no elements of finite order, and its rank is equal to the rank of the group G. Moreover, X' is the character group of the group G^*. We shall now show that the dimension of the group X' is not less than the rank of the group G^*. This will complete our investigation.

Let

$$x_1, \cdots, x_n, \cdots \tag{5}$$

be a complete system of linearly independent elements of the group G^*. Then every element x of the group G^* can be expressed linearly in terms of the elements of the system (5) with rational coefficients (since G^* contains no elements of finite order, division in G^* is always unique, although not always possible). Let

$$d_1, \cdots, d_n, \cdots \tag{6}$$

be a finite system of real numbers. Starting with the system (6) we define the character α of the group G^*. Let $x = \sum_{i=1}^{n} r_i x_i$, and let $\alpha(x) = \sum_{i=1}^{n} r_i d_i$, where the right side is considered as an element of the group K, i.e., it is reduced modulo 1. The character α, defined in this way, depends on n real parameters and therefore the group X' is at least n-dimensional (see §44, B), C)). But n is an arbitrary number not exceeding the number of elements of the sequence (5), i.e., n is an arbitrary number not exceeding the rank of the group G^*. Hence the dimension of the group X is not less than the rank of the group G^*, and hence not less than the rank of the group G. In conjunction with what we have proved above we see that the dimension of the group X is equal to the rank of the group G.

Example 50. Let G be a discrete group with two linearly independent generators a and b. We denote by D the additive topological group of real numbers. We define the law of multiplication of the elements of the group G by the elements of the group D (see Definition 36), starting with two real numbers α and β whose ratio α/β is irrational. The product of the element $x = ma + nb \in G$ by the element $d \in D$ is defined by letting $xd = dm\alpha + dn\beta$, where the right side is considered as an element of the group K, i.e., is reduced modulo 1. It can readily be seen that the law of multiplication thus defined satisfies the distributive laws and any natural continuity conditions. Fur-

thermore, the groups G and D are orthogonal in the sense of Definition 36. In fact $xd = d(m\alpha + n\beta)$ can be equal to zero (mod 1) for every $d \varepsilon D$ only if $x = 0$. Moreover, if $d \varepsilon (D, G)$, we have $d\alpha = 0$, $d\beta = 0$ (of course we understand here equations with respect to the modulus 1, so that in the usual numerical notation these equalities should be written as follows: $d\alpha = m$, $b\beta = n$, where m and n are integers). But this is impossible if $d \neq 0$, since the ratio α/β is by assumption irrational.

It is obvious, however, that neither of the groups G and D is the character group of the other. Hence Theorem 38 is not true for general locally compact groups.

EXAMPLE 51. Let $\alpha_1, \cdots, \alpha_r$ be a finite system of linearly independent irrational numbers, i.e., such that a sum $n_1\alpha_1 + \cdots + n_r\alpha_r$ with integral coefficients can be an integer only if all of its coefficients are equal to zero. We shall show that for any ϵ and any system of real numbers $d_1, \cdots, d_r$ a system of integers $n_1, \cdots, n_r$ and an integer m can be found such that

$$|m\alpha_i - d_i - n_i| < \epsilon, \qquad i = 1, \cdots, r.$$

This proposition is an elementary theorem in the theory of approximations of real numbers by integral multiples of irrationals. We shall prove it here by use of the theory of characters. This proof is of interest since the original exposition of the theory of characters depended on the above theorem in the theory of irrational numbers.

Let G be a discrete group with r linearly independent generators $a_1, \cdots, a_r$. We associate with every integer m a character β_m of the group G in the following way: if $x = n_1a_1 + \cdots + n_ra_r$ then we shall define $\beta_m(x) = m(n_1\alpha_1 + \cdots + n_r\alpha_r)$, where the right side is considered as an element of the group K, i.e., is reduced modulo 1. It can readily be seen that $\beta_m + \beta_n = \beta_{m+n}$. Hence the set A of all the characters of the type β_m forms a group. We denote by X the character group of the group G. Then A is a subgroup of the abstract group X. We denote by Φ the closure of the set A in X. It can be seen easily that if $\beta_m(x) = 0$ for every m, then $x = 0$. This follows from the linear independence of the numbers α_i. We can conclude from this that $(G, \Phi) = \{0\}$, and this gives us by Theorem 33 the equality $\Phi = X$. Hence the set A is everywhere dense in X, i.e., every character β of the group G can be approximated arbitrarily closely by characters of the form β_m. The proof of the theorem now follows directly from the above statement. In fact if $d_1, \cdots, d_r$ are given numbers, we can define a character β of the group G by setting $\beta(a_i) = d_i$, $i = 1, \cdots, r$, where the right side is considered as an element of the group K. By approximating the character β by the characters β_m we get the desired relations.

34. The Direct Sum for a Group and for its Character Group

The connection between a group G and its character group X which we have established in the preceding section in case G is compact or discrete enables us

to associate with every decomposition of the group G into a direct sum a definite decomposition of the group X into a direct sum (see Definitions 10* and 29). This question has already been considered in Theorem 36 for a finite number of summands only. Here we shall consider this question simultaneously for a finite and an infinite number of summands, but we shall have to confine ourselves to compact and discrete groups.

A) Let G be a compact or discrete group, X its character group, and M a set of subgroups of the group G. We denote by Ω the totality of all the subgroups of the group X of the form (X, H), where $H \varepsilon M$, by L the minimal subgroup of the group G which contains all the groups of the set M, and by Ψ the intersection of all the subgroups of the set Ω. Then we have

$$\Psi = (X, L), \tag{1}$$

or what is the same,

$$L = (G, \Psi). \tag{2}$$

It follows from Theorem 33 (see Theorem 37) that M is composed of all the groups of the form (G, Φ), where $\Phi \varepsilon \Omega$. Let

$$\Psi' = (X, L) \tag{3}$$

and

$$L' = (G, \Psi). \tag{4}$$

For every $H \varepsilon M$ we have $H \subset L$, and therefore $(X, H) \supset (X, L) = \Psi'$, i.e.,

$$\Psi \supset \Psi'. \tag{5}$$

Furthermore, for every $\Phi \varepsilon \Omega$ we have $\Phi \supset \Psi$ and hence $(G, \Phi) \subset (G, \Psi)$ i.e.,

$$L \subset L'. \tag{6}$$

From Theorem 33 we have $\Psi = (X, L')$, and since $L \subset L'$, it follows that $(X, L) \supset (X, L')$, i.e., $\Psi' \supset \Psi$. The last relation together with (5) gives $\Psi' = \Psi$. Hence A) is established.

THEOREM 39. *Let G be a compact or discrete group and X its character group. Let us suppose that G decomposes into the direct sum of a countable or finite system of its subgroups $H_1, \cdots, H_n, \cdots$. Then there exists one and only one decomposition of the group X into a direct sum of subgroups $\Phi_1, \cdots, \Phi_n, \cdots$ which satisfies the following conditions:*

a) *For $i \neq j$, we have*

$$\Phi_i \subset (X, H_j), \tag{7}$$

or what is the same,

$$H_j \subset (G, \Phi_i). \tag{8}$$

b) *The groups H_i and Φ_i form an orthogonal pair by virtue of the same law of multiplication which holds for the groups G and X* (see Definition 36). *Hence the groups H_i and Φ_i are character groups of each other* (see Theorem 38).

Proof. Let us denote by L_k the minimal subgroup of the group G which contains all the subgroups H_i with the exception of H_k. We denote by H'_k the intersection of all the subgroups L_i with the exception of the group L_k. It is obvious that $H_i \subset H'_i$. We shall show that $H_i = H'_i$.

Since by assumption the intersection of all subgroups L_i (see Definitions 10* and 29) contains only zero, it follows that the intersection $H'_i \cap L_i$ also contains only zero. Since G can be decomposed into the direct sum of the groups H_i and L_i (see §5, A*) and §21, A)) it follows that $H_i + L_i = G$ and hence $H'_i + L_i = G$, and G is decomposable into the direct sum of the groups H'_i and L_i. Suppose there exists an element $z \varepsilon H'_i$, which does not belong to H_i. Then, since G is decomposable into the direct sum of the subgroups H_i and L_i, $z = x + y$, where $x \varepsilon H_i$, and $y \varepsilon L_i$. We also have $x \varepsilon H_i$, $y \varepsilon L_i$, and $z = z + 0$, where $z \varepsilon H'_i$, $0 \varepsilon L_i$. Hence if G is considered as the direct sum of the group H'_i and L_i we get two decompositions of the element z: $z = z + 0 = x + y$, therefore $z = x$, i.e., $z \varepsilon H_i$, and $H'_i = H_i$.

Let us now take $\Phi_i = (X, L_i)$, $\Psi_i = (X, H_i)$. It follows from Theorem 37 and proposition A), that Ψ_k is the minimal subgroup containing all the subgroups Φ_i with the exception of Φ_k, and Φ_k is the intersection of all the subgroups Ψ_i with the exception of Ψ_k. Since the minimal subgroup containing all the groups H_i coincides with G, the intersection of all the subgroups Ψ_i contains only zero (see A)). Furthermore, since the intersection of all the subgroups L_i contains only zero, the minimal subgroup containing all the subgroups Φ_i coincides with X. Hence X is decomposable into the direct sum of the subgroups $\Phi_1, \cdots, \Phi_n, \cdots$.

Relations (7) and (8) are obvious. Let us show that H_i and Φ_i form an orthogonal pair. Let $x \varepsilon H_i$, $x \neq 0$: then there is an element $\gamma \varepsilon X$ such that $\gamma(x) \neq 0$. Let $\gamma = \alpha + \beta$, where $\alpha \varepsilon \Phi_i$, and $\beta \varepsilon \Psi_i$. Since $\Psi_i = (X, H_i)$, it follows that $\beta(x) = 0$, and hence $\alpha(x) = \gamma(x) \neq 0$. We therefore get $(H_i, \Phi_i) = \{0\}$. In view of the complete symmetry of the relations, we can prove in an analogous way that $(\Phi_i, H_i) = \{0\}$. Hence the groups H_i and Φ_i are orthogonal.

Suppose now that there exists another decomposition of the group X into a direct sum of subgroups $\Phi'_i, \cdots, \Phi_n, \cdots$ satisfying condition a), i.e., such that for $i \neq j$ we have $\Phi'_i \subset (X, H_j)$. It follows from this relation that $\Phi'_i \subset \Psi_j$ for $i \neq j$, i.e., $\Phi_i \subset \Phi_i$. Let is now denote by Ψ'_k the minimal subgroup containing all the subgroups Φ'_i with the exception of Φ'_k. Then $\Psi'_i \subset \Psi_i$. Since $\Phi'_i + \Psi'_i = X$, it follows that $\Phi'_i + \Psi_i = X$. Since the intersection $\Phi_i \cap \Psi_i$ contains only zero, the intersection $\Phi'_i \cap \Psi_i$ also contains only zero. Hence G is decomposable into the direct sum of the subgroups Φ'_i and Ψ_i. We have here exactly the same state of affairs as in the beginning of the proof of this

theorem. Just as we proved there that $H'_i = H_i$, so we can show here that $\Phi'_i = \Phi_i$. This proves the uniqueness of the decomposition of the group X into a direct sum satisfying condition a). This completes the proof of Theorem 39.

Theorem 39 shows that the study of the decomposition of the group X into a direct sum is entirely equivalent to the study of the decomposition of the group G into a direct sum.

The primary value and interest of Theorem 39 consists in the reduction of the problem of decomposition of a compact commutative group into a direct sum to the same problem for a discrete commutative group.

35. Locally Compact Groups

It was shown in the preceding section that every compact commutative group is the character group of a discrete group. We have given in this way a method of construction of a general compact commutative group, and its study has been reduced to the study of a discrete group. We have now before us the problem of proving Theorem 32 for locally compact groups. Before attempting to do this, however, we have to make a rather detailed investigation of the structure of locally compact commutative groups. Lemma 1 (see below) enables us to reduce the study of locally compact commutative groups to that of compact groups, which we have already investigated. It turns out that fundamentally a locally compact, commutative group differs from a compact group only by a vector direct summand (see Theorem 41 and Remark E)).

LEMMA 1. *Let G be a locally compact, commutative, connected, but not compact group. Then there exists in G a discrete subgroup D having a finite system of linearly independent generators* (see §6, B)), *such that the factor group G/D is compact.*

In order to prove Lemma 1 we shall first prove the following lemma.

LEMMA 2. *Let G be a connected, commutative, locally compact, but not compact group, and U a symmetric neighborhood of zero of the group G i.e., such that $-U = U$, for which the closure $\overline{U}$ is compact. Then there exists an element d in the boundary $U' = \overline{U} - U$ of the open set U such that the relation $nd \in U$, where n is an integer, implies that $n = 0$. In this way the element d generates a discrete infinite cyclic subgroup of the topological group G.*

PROOF. Let $U_1 = U$, and define U_{n+1} by induction from (see §2, A))

(1) $$U_{n+1} = U_n + U.$$

Since U is open, U_n is also open (see §16, C)). It can be seen easily that

(2) $$U_r + U_s = U_{r+s}$$

and

(3) $$\overline{U}_r + \overline{U}_s = \overline{U}_{r+s}.$$

Since $\bar{U}$ is compact, U_n is also compact (see §16, G)). Let

(4) $$U_n' = \bar{U}_n - U_n.$$

Since $\bar{U}_n$ is compact, it follows that $\bar{U}_n \neq G$, and since G is connected we can conclude that U_n' is not empty.

We shall show that

(5) $$U_r + \bar{U}_s = U_{r+s}.$$

In fact let $a \varepsilon U_r$, and $b \varepsilon \bar{U}_s$. Since b is a limit element of U_s, there exists an arbitrarily small element c such that $b - c \varepsilon U_s$ (c is arbitrarily small in the sense that it can be selected from an arbitrary neighborhood of zero). Since c is arbitrarily small, we can suppose that $a + c \varepsilon U_r$, since U_r is open. Then we have

$$a + b = (a + c) + (b - c) \varepsilon U_{r+s}.$$

(see (2)). Hence $U_r + \bar{U}_s \subset U_{r+s}$. It is obvious that $U_r + \bar{U}_s \supset U_{r+s}$.

We now construct an infinite sequence

(6) $$d_1, \cdots, d_n, \cdots$$

of elements of the set $\bar{U}$ such that

(7) $$d_1 + \cdots + d_n \varepsilon U_n'$$

for every n. Since U_n' is not empty, there exists an element $c_n \varepsilon U_n'$. From (3) this element c_n can be written in the form

(8) $$c_n = d_{1,n} + \cdots + d_{n,n},$$

where $d_{i,n} \varepsilon \bar{U}$, $i = 1, \cdots, n$. We shall show that for $j < n$,

(9) $$g = d_{1,n} + \cdots + d_{j,n} \varepsilon U_j'.$$

In fact let $h = c_n - g$. Obviously $g \varepsilon \bar{U}_j$, $h \varepsilon \bar{U}_{n-j}$, but since $g + h = c_n \varepsilon U_n'$, it follows from (5) that $g \varepsilon U_j'$. Since $\bar{U}$ is compact, we can make use of the diagonal process (see Theorem 9) to select a sequence of integers $n_1, \cdots, n_k, \cdots$ such that the limit

(10) $$\lim_{k \to \infty} d_{i,n_k} = d_i$$

exists for every i. We shall show that

(11) $$d_1 + \cdots + d_j \varepsilon U_j'$$

for every j. In fact

$$d_1 + \cdots + d_j = \lim_{k \to \infty} \{d_{1,n_k} + \cdots + d_{j,n_k}\}$$

(see (10)), but since the sum under the limit sign in the last relation belongs

to U'_j (see (9)), the left side also belongs to U'_j, since U'_j is closed. Hence the sequence (6) is constructed.

We shall now show that for an arbitrary system

(12) $$m_1, \cdots m_r$$

of distinct integers we have

(13) $$a = d_{m_1} + \cdots + d_{m_r} \varepsilon U'_r.$$

Let n be an integer exceeding all the numbers of the system (12). Then the sum

(14) $$c = d_1 + \cdots + d_n$$

can be written in the form $c = a + b$. Obviously $b \varepsilon \overline{U}_{n-r}$ and $a \varepsilon \overline{U}_r$. Since moreover, $a + b \varepsilon U'_n$ (see (7)), it follows that $a \varepsilon U'_r$ (see (5)).

Let d be a limit point of the sequence (6). We shall show that

(15) $$rd \varepsilon U'_r$$

for an arbitrary positive integer r.

Let V be a neighborhood of the element rd. We denote by W a neighborhood of the element d such that

(16) $$rW \subset V.$$

Since the element d is a limit element for the sequence (6), there exists in the neighborhood W a system of elements $d_{m_1}, \cdots, d_{m_r}$, all of whose indices are distinct. It follows from (13) that

(17) $$a = d_{m_1} + \cdots + d_{m_r} \varepsilon U'_r.$$

Hence an arbitrary neighborhood V of the element rd intersects U'_r since $a \varepsilon V$ (see (16) and (17)). But the set U'_r is closed and therefore $rd \varepsilon U'_r$.

Since U'_r does not intersect U for any value of r, the element rd cannot belong to U for any positive integer r (see (15)). Therefore since the neighborhood U is symmetric, no element nd, where n is an integer, belongs to U with the single exception of $0 \cdot d$.

Hence Lemma 2 is established.

Proof of Lemma 1. Let U be a symmetric neighborhood of zero of the group G, i.e., $-U = U$, for which the closure $\overline{U}$ is compact. We shall construct by induction the system

(18) $$\Delta_r = \{a_1, \cdots, a_r\}$$

of elements of the group G satisfying the following conditions: a) The linear form $n_1a_1 + \cdots + n_ra_r$ with integral coefficients belongs to U only if $n_i = 0$, $i = 1, \cdots, r$, and b) $a_i \varepsilon U'$, $i = 1, \cdots, r$.

We denote by D_r the set of all linear forms

$$(19) \qquad n_1a_1 + \cdots + n_ra_r$$

with integral coefficients, and show that if the system (18) satisfies conditions a) and b), then the set D_r is a discrete subgroup of the group G having the system of linearly independent generators (18). First, it is clear that the set D_r is a subgroup of the abstract group G. Furthermore, it follows from condition a) that if $n_1a_1 + \cdots + n_ra_r = 0$, then $n_i = 0$, $i = 1, \cdots, r$, and this means that the system (18) is a linearly independent system of generators of the group D_r. Since the neighborhood U contains only the zero element of the group D_r, the group D_r is closed in the topological space G and is a discrete subgroup of the group G.

We note that from Lemma 2 the system of elements (18) satisfying conditions a) and b) exists for $r = 1$. Supposing that the system (18) has been constructed for $r = s$, we show that there are two possible cases: 1) the factor group G/D_s is compact, in which case Lemma 1 has already been proved, and 2) the system (18) constructed for $r = s$ can be enlarged to the system with $r = s + 1$ by adjoining one element.

Let us suppose that the first case does not occur, i.e., that the factor group $G^* = G/D_s$ is not compact. Let f be the natural homomorphic mapping of the group G on the group G^* (see §19, C)). From the construction of the neighborhoods in the factor group G^* (see Definition 24), $f(U) = U^*$ is a neighborhood of zero of the group G^*. Since U is symmetric, U^* is also symmetric, i.e., $-U^* = U^*$. Since

$$(20) \qquad \overline{U}^* \subset f(\overline{U}),$$

$\overline{U}^*$ is compact. We shall show that

$$(21) \qquad U'^* \subset f(U').$$

In fact $\overline{U}^* \subset f(U) \cup f(U')$ (see (20)). Subtracting from both sides of this relation the set $U^* = f(U)$ we get $U'^* \subset f(U')$. We now apply Lemma 2 to the group G^* and its neighborhood U^*. Let d^* be such an element of U'^* that

$$(22) \qquad nd^* \in U^* \quad \text{implies} \quad n = 0.$$

We now denote by a_{s+1} an element of U' such that $f(a_{s+1}) = d^*$. This element exists because of relation (21). It can readily be seen that the system $a_1, \cdots, a_s, a_{s+1}$ satisfies conditions a) and b). It is obvious that b) is satisfied since $a_{s+1} \in U'$. Let us suppose that

$$(23) \qquad a = n_1a_1 + \cdots + n_sa_s + n_{s+1}a_{s+1} \in U.$$

Then $f(a) = n_{s+1}d^* \in U^*$ and hence by (22), $n_{s+1} = 0$. Thus the linear form (23) becomes $a = n_1a_1 + \cdots + n_sa_s$. But if $a \in U$, then $n_i = 0$, $i = 1, \cdots, s$, since condition a) is satisfied for the system Δ_s by assumption.

Hence we can enlarge the system Δ_r by induction as long as the group G/D_r is not compact. But an unlimited enlargement is not possible since U' is com-

pact, and it follows, from condition a) in particular, that the difference $a_i - a_j$, where $i \neq j$, cannot belong to U.

Hence Lemma 1 is proved.

THEOREM 40. *Let G be a locally compact group, G' the component of zero of the group G* (see §22, A)), *and U a neighborhood of zero of the group G. If the factor group G/G' is compact, there exists a compact subgroup $Q \subset U$ of the group G such that the factor group G/Q decomposes into the direct sum of a toroidal group T* (see §32, K)), *a vector group A, and a finite group C.*

To prove Theorem 40, we first prove the two following propositions A) and B).

A) Let G be a locally compact commutative connected group and D a discrete subgroup of G having a finite system of linearly independent generators. If the factor group G/D is a toroidal group T^*, then the group G can be decomposed into the direct sum of a vector group A and a toroidal group T.

The group T^*, being toroidal, decomposes into the direct sum of a finite number r of groups isomorphic with K (see §32, K)). In this way T^* can be thought of as a factor group A^*/N, where A^* is the vector group of dimension r, and N is composed of all the vectors of the group A^* with integral components. We denote the natural homomorphic mapping of the group A^* on the group T^* by f, and the natural homomorphic mapping of the group G on T^* by g. Since the groups D and N are discrete, the mappings f and g are one-to-one in small neighborhoods of zero, and therefore we can define uniquely the mapping

$$g^{-1}(f(x)) = h(x) \tag{24}$$

of a neighborhood U of zero of the group A^* on a neighborhood V of zero of the group G. The mapping h is a local isomorphism of the group A^* in G (see Definition 30).

We now extend the local isomorphism h of the group A^* on the group G into a homomorphism h' of the whole group A^* on the whole group G. Let x be an arbitrary element of the group A^*. There exists a sufficiently large number n such that $x/n \in U$, and we let $h'(x) = nh(x/n)$. It can readily be seen that h' is defined by this relation uniquely and that it represents a homomorphic mapping of the group A^* on the group G. Furthermore, it follows from (24) that

$$f(x) = g(h'(x)). \tag{25}$$

Let us denote by N' the kernel of the homomorphism h'. It follows from (25) that $N' \subset N$. It is also not hard to see that the factor group N/N' is isomorphic with the group D. Since the factor group N/N' contains no elements of finite order (see §6, A)), we can select a system of linearly independent generators

$$a_1, \cdots, a_s, a_{s+1}, \cdots, a_r \tag{26}$$

of the group N in such a way that $a_1, \cdots, a_s$ form a system of generators of the

group N'. In fact by E) of §6, we can select in N a system of linearly independent generators (26) in such a way that the elements $d_1a_1, \cdots, d_sa_s$, where $d_i > 0$, $i = 1, \cdots, s$, and d_{i+1} is divisible by d_i, $i = 1, \cdots, s - 1$, form a system of generators of the group N'. It can readily be seen that since the factor group has no elements of finite order, then all the d_i must be equal to unity. The vectors of the system (26) can be taken for a basis of the vector space A^*. Making use of this choice of basis, it becomes obvious that the factor group $A^*/N' = G$ can be decomposed into the direct sum of s groups isomorphic with the group K and $r - s$ groups isomorphic with the additive group of real numbers. Hence G decomposes into the direct sum of an s-dimensional toroidal T and the $(r - s)$-dimensional vector group A, which proves A).

B) Let G be a locally compact commutative group, G' the component of zero of the group G, and D a discrete subgroup of the group G' having a finite system of linearly independent generators. If the factor group G/D is a generalized toroidal group, then the group G decomposes into the direct sum of a vector group A and a generalized toroidal group T (see §32, J)).

It can readily be seen that G'/D is the component of zero of the group G/D, and since the group G/D is a generalized toroidal group, the group G'/D is a toroidal group (see §33, K)). Therefore the group G' decomposes by A) into the direct sum of a vector group A and a toroidal subgroup T'.

Since it follows from what we have just said that the group G/G' is finite, it can be decomposed into the direct sum of a finite number of finite cyclic groups $Z_1, \cdots, Z_k$ (see §6, F)). We denote the generator of the group Z_i by z_i^*, and an element of the coset z_i^* by z_i. If r_i is the order of the group Z_i, then $r_iz_i \in G'$, and G' contains an element x_i such that $r_ix_i = r_iz_i$, since division is always possible in the group G, which is a direct sum of a vector group and a toroidal group. Let $z_i' = z_i - x_i$, then $r_iz_i' = 0$. The subgroup C of the group G having $z_1', \cdots, z_k'$ for generators can easily be seen to be finite, and the group G decomposes into the direct sum of the subgroups G' and C. And since G' in turn decomposes into the direct sum of A and T', proposition B) follows from remark K) of §32.

Proof of Theorem 40. Let D be a discrete subgroup of the group G' having a finite system of linearly independent generators and such that the factor group G'/D is compact (see Lemma 1). Since the factor group G/G' is compact by assumption, and since the factor group G'/D is also compact, the factor group $G/D = G^*$ is compact (see §18, F)). Let us denote by f the natural homomorphic mapping of the group G on the group G^*. Since the subgroup D is discrete, there exists a sufficiently small symmetric neighborhood V of zero of the group G such that the neighborhood $4V$ contains only the zero element of the group D. We shall also suppose that $\overline{V}$ is compact and belongs to U.

By Theorem 37 the compact group G^* is the character group of some discrete group X. Let $H_1, \cdots, H_n, \cdots$ be an increasing sequence of subgroups of the group X, which exhausts the group X, and is such that each H_n admits a finite system of generators. Let $Q_n^* = (G^*, H_n)$. It can readily be seen that

for a sufficiently large m we have $Q_m^* \subset f(V)$ (the proof of this is similar to the proof of remark A) of §33). Then the factor group G^*/G_m^*, being the character group of the group H_m, is a generalized toroidal group (see §32, J)). Let us denote by Q the complete inverse image of the group Q_m^* in $\overline{V}$ under the mapping f. It follows that Q is a compact subgroup of the group G, whose intersection with D contains only zero. We shall prove only that Q is a subgroup, the rest being evident. Let a and b be two elements of Q; then $f(a - b) = f(a) - f(b) \varepsilon Q_m^*$, and there exists an element $c \varepsilon Q$, such that $f(c) = f(a - b)$, i.e., $f(a - b - c) = 0$, or what is the same, $a - b - c \varepsilon D$. Since, moreover, $a - b - c \varepsilon 3\overline{V} \subset 4V$, it follows that $a - b - c = 0$, i.e., $a - b = c \varepsilon Q$. Hence Q is a group. We note that the complete inverse image of the group Q_m^* in the group G under the mapping f is $D + Q$. Hence the factor group $G/(D + Q)$ is isomorphic with the factor group G^*/Q_m^* (see §19, E)). We denote the factor group G/Q by H and the image of the group $D + Q$ in the group H under the corresponding homomorphism by E. Then the factor group H/E is isomorphic with the factor group $G/(D + Q)$ (see §19, E)). Since, furthermore, $D \cap Q$ contains only zero, E is isomorphic with D (see Theorem 14). Hence the group H contains the discrete subgroup E having a finite system of linearly independent generators and such that the factor group H/E, which is isomorphic with the factor group G^*/Q_m^*, is a generalized toroidal group. Hence by B) the group H decomposes into the direct sum of a vector group A and a generalized toroidal group T'. Hence Theorem 40 follows from remark K) of §32.

C) Let G be a locally compact commutative group and G' the component of zero of the group G. If the factor group G/G' is compact then there exists in G a compact subgroup Z such that the factor group G/Z is a vector group. The subgroup Z is the maximal compact subgroup of the group G in the sense that all other compact subgroups of the group G are contained in Z. In this way Z is defined uniquely.

Let Q be a compact subgroup of the group G such that the factor group $G/Q = G^*$ can be decomposed into the direct sum of a vector subgroup A and a generalized toroidal subgroup T (see Theorem 40). We denote by Z the complete inverse image of the group T in the group G. Since the groups T and Q are compact, the subgroup Z is also compact (see §18, F)). Furthermore, the factor groups G/Z and G^*/T are isomorphic (see §19, E)). But since the factor group G^*/T is obviously isomorphic with the vector group A (see Theorem 14), it follows that the factor group G/Z is also isomorphic with the vector group A, and the first point of proposition C) is proved for the subgroup Z.

Let now Z' be an arbitrary compact subgroup of the group G. Under the homomorphism of G in G/Z, the group Z' maps into a compact subgroup of the vector group A. But the vector group contains only one compact subgroup, namely the null subgroup. Hence under the homomorphism of G in G/Z the subgroup Z' maps into a null group and hence $Z' \subset Z$. This proves the second point of proposition C) for the group Z.

D) If a locally compact commutative group G admits a compact subgroup Z such that the factor group $G/Z = G^*$ is a connected group, then the group G satisfies the conditions of remark C), i.e., the factor group G/G', where G' is the component of zero of the group G, is compact.

Let $H = G' + Z$. Since Z is compact, H is a subgroup of the group G (see §20, D)). We shall show that $G = H$. To do this we prove that G/H contains only zero. Let $G/G' = G^{**}$, and denote by H^{**} the image of the group H in G^{**}. Then the groups G/H and G^{**}/H^{**} are isomorphic (see §19, E)). Furthermore, the group G^{**} is a 0-dimensional group (see §22, C)). But then the group G^{**}/H^{**} is also a 0-dimensional group. In fact, the group G^{**} contains an arbitrarily small open compact subgroup Q^{**} (see Theorem 17). The image of the group Q^{**} in the group G^{**}/H^{**} is also an arbitrarily small open compact subgroup, and, therefore, G^{**}/H^{**} is a 0-dimensional group (see §22, G)). Hence the group G/H is a 0-dimensional group. On the other hand, the group G/H is isomorphic with some factor group of the group G/Z (see §19, E)), i.e., G/H is connected. Being both connected and 0-dimensional, the group G/H contains only zero. Hence $H = G$.

It follows that the factor group G/G' is isomorphic with the factor group Z/Z', where Z' is the intersection $G' \cap Z$ (see Theorem 14). And since Z is compact, G/G' is also compact (see §18, E)).

Remark C) leads us naturally to the following theorem, which plays an important part in what follows.

THEOREM 41. *Let G be a locally compact commutative group and G' the component of zero of the group G. If the factor group G/G' is compact, then the group G decomposes into the direct sum of a compact subgroup Z and a vector subgroup A. Here the compact subgroup Z is defined uniquely, while the vector subgroup A is arbitrary, except that its dimension is determined by the group G.*

PROOF. Let Z be the maximal compact subgroup of the group G (see C)). We denote by

$$(27) \qquad U_1, \cdots, U_n, \cdots$$

a decreasing sequence of neighborhoods of zero of the group G which is such that the closure $\overline{U}_n$ of every neighborhood U_n is compact and the intersection of all $\overline{U}_n$ contains only the zero of the group G. We shall now construct by induction the sequence of subgroups

$$(28) \qquad G_0 = G, G_1, \cdots, G_n,$$

satisfying the following conditions: a) $G_{n+1} \subset G_n$, b) the intersection $Z \cap G_n \subset U_n$, c) the group sum $Z + G_n = G$, and d) the groups G_n satisfy the condition of remark C).

The first member of the sequence (28) is the group G. Let us suppose that all the groups up to and including G_n have already been constructed. We then construct the group G_{n+1}.

By Theorem 40 there exists a compact subgroup $Q_n \subset U_{n+1}$ of the group G_n such that the factor group G_n/Q_n decomposes into the direct sum of a vector group A_n and a generalized toroidal group T_n. We denote the inverse image of the group T_n in the group G_n by Z_n, and the inverse image of A_n by G_{n+1}. Obviously G_{n+1}/Q_n is isomorphic with A_n, i.e., it is connected, and therefore by D), the group G_{n+1} satisfies the conditions of remark C). Hence condition d) holds for the group G_{n+1}. Furthermore,

$$G_{n+1} \cap Z_n = Q_n \tag{29}$$

and since obviously $G_{n+1} + Z_n = G_n$, it follows from Theorem 14 that G_n/Z_n is isomorphic with the vector group A_n. Hence Z_n is the maximal compact subgroup of the group G_n (see C)). Then the intersection $G_{n+1} \cap Z$, being a compact subgroup of the group G_n, belongs to Z_n and hence

$$G_{n+1} \cap Z \subset G_{n+1} \cap Z_n \subset Q_n \subset U_{n+1} \tag{30}$$

(see (29)). Hence condition b) holds for the group G_{n+1}. By the hypothesis of the induction $G = G_n + Z$; but $G_n = G_{n+1} + Z_n$ and therefore

$$G = G_{n+1} + Z_n + Z = G_{n+1} + Z, \tag{31}$$

since Z_n, being a compact subgroup of the group G, must be contained in Z (see C)). Hence the group G_{n+1} satisfies the condition of C). Since condition a) is automatically satisfied, the induction is completed and we can assume the existence of the whole sequence (28).

We now denote by A the intersection of all the subgroups (28) and show that G is decomposable into the direct sum of the subgroup Z and the subgroup A (see Definition 28).

It follows from condition b) that the intersection of Z and A contains only zero. We shall show that $Z + A = G$. In fact let x be an arbitrary element of the group G. Then by condition c), $x = z_n + a_n$, where $z_n \in Z$, $a_n \in G_n$. Since the group Z is compact, we can select from the sequence of elements z_n, a subsequence which converges to an element $z \in Z$. Then the corresponding subsequence of elements of A_n will converge to the element $x - z = a$, and we have $x = z + a$. Since the sets G_n are closed, it follows that $a \in A$. Hence $G = Z + A$ and all the conditions of Definition 28 are satisfied.

The subgroup A is isomorphic with the factor group G/Z, and since the latter is a vector group, it follows that A also is a vector group.

This proves Theorem 41.

Theorem 41 analyzes the structure of a rather wide class of locally compact groups. The following remark shows the relation of this class to general locally compact groups.

E) Let G be an arbitrary locally compact commutative group. Then there exists a subgroup H in G satisfying the following conditions: a) the factor group G/H is discrete, b) the factor group H/H', where H' is the component of

zero of the group H, is compact. In this way the group H satisfies the conditions of Theorem 41.

Let us denote by G' the component of zero of the group G. Then the factor group $G/G' = G^*$ is a 0=dimensional group (see §22, C)). By Theorem 17, the group G^* contains an open compact subgroup H^*. We denote the inverse image of the subgroup H^* in the group G by H. Then the factor group G/H is isomorphic with the factor group G^*/H^* (see §19, E)), and since the latter is discrete, G/H must also be discrete. Furthermore, since the factor group G/H is discrete, the component of zero H' of the group H coincides with the component of zero of the group G, and H/H' is isomorphic with H^*, which is compact by assumption. In this way E) is proved.

We now pass to the proof of the fundamental theorem of the theory of characters for general locally compact groups. To do this we first prove the following proposition;

F) Let G be an arbitrary locally compact commutative group. Then there exists in G an expanding sequence of subgroups

$$H_1, \cdots, H_n, \cdots \tag{32}$$

which comprises the whole group G, and which satisfies the following conditions: a) the factor group G/H_n is discrete, b) every group H_n decomposes into the direct sum of a vector group A_n, a compact group Z_n, and a discrete group D_n having a finite system of linearly independent generators.

Let H be the subgroup of the group G which we have constructed in remark E). Since the factor group $G^* = G/H$ is discrete, it contains an expanding sequence of subgroups

$$H_1^*, \cdots, H_n^*, \cdots \tag{33}$$

which comprises the whole group G^*, and is such that every group H_n^* admits a finite system of generators. We denote the inverse image of the group H_n^* in the group G by H_n, and we shall show that H_n is decomposable into the sum of three groups as indicated. The fact that the factor group G/H_n is discrete is obvious, since $H \subset H_n$ and G/H is discrete.

The group H_n^* can be decomposed into the direct sum of a finite group C_n^* and a group D_n^* having a finite system of linearly independent generators $a_1^*, \cdots, a_r^*$ (see §6, F)). We denote the inverse image of the group C_n^* in the group G by C_n. Then the factor group C_n/H is isomorphic with the group C_n^* and hence it is finite. Therefore the group C_n satisfies the conditions of Theorem 41, since the group H satisfies these conditions. Hence the group C_n decomposes into the direct sum of a vector group A_n and a compact group Z_n. We denote by a_i one of the inverse images of the element a_i^* in the group G, $i = 1, \cdots, r$, and by D_n the subgroup of the abstract group G with the generators $a_1, \cdots, a_r$. It is not hard to see that D_n is a discrete subgroup of the group G, and that H_n decomposes into the direct sum of the groups C_n and D_n.

But since we have just shown that the group C_n decomposes into the direct sum of the group A_n and Z_n the proposition F) is proved.

PROOF OF THEOREM 32. This proof depends on remark C) of §31. Let

$$H_1, \cdots, H_n, \cdots \tag{34}$$

be the sequence of subgroups of the group G constructed in proposition F). We denote by X_n the character group of the group H_n. Since the group H_n decomposes into the direct sum of three groups for each of which Theorem 32 has already been proved (see §32, J) and L), and §33, D)), it follows from Theorem 36 that the group H_n is the character group of the group X_n. Therefore every non-zero element $x \in H_n$ is a non-zero character of the group X_n, i.e., there exists an element $\beta \in X_n$ such that

$$x(\beta) = \beta(x) \neq 0. \tag{35}$$

We shall show that condition a) of remark C) of §31 holds for the group G. Let x be an element different from zero of the group G. Since the sequence (34) comprises the whole group G, there exists a number n such that $x \in H_n$. From relation (35) there exists a character β of the group H_n such that $\beta(x) \neq 0$. Since the factor group G/H_n is discrete, the character β can be extended into a character α of the whole group G (see Lemma of §32) and therefore we have $\alpha(x) \neq 0$.

We shall now show that condition b) of remark C) of §31 is also satisfied for the group G. Let X be the character group of the group G, and let $\Phi_n = (X, H_n)$ (see Definition 35). By Theorem 34, the group G/H_n has the group Φ_n for its character group, and since G/H_n is discrete, the group Φ_n is compact (see Theorem 31). Since the sequence (34) is an increasing sequence, the sequence

$$\Phi_1, \cdots, \Phi_n, \cdots \tag{36}$$

is decreasing. Also since the sequence (34) comprises the whole group G, the intersection of all the groups of the sequence (36) contains only the zero of the group X. It follows from this that there exists for every neighborhood V of zero of the group X a sufficiently large number m such that

$$\Phi_m \subset V. \tag{37}$$

Let now x be an arbitrary character of the group X and let U be that neighborhood of zero of the group K which we have discussed in remark B) of §30. Furthermore, let V be a neighborhood of zero of the group X such that $x(V) \subset U$. We then have $x(\Phi_m) \subset U$ (see (37)), and hence $x(\Phi_m) = \{0\}$ (see §30, B)). Therefore the character x of the group X can be considered as a character of the factor group X/Φ_m (see Theorem 34). It follows from remark M) of §32 that the factor group X/Φ_m is the character group of the group H_m, i.e., $X_m = X/\Phi_m$. From what we have mentioned before H_m is in turn the character group of the group X_m and therefore $x \in H_m$, and this means that x, being a character of the group X, belongs to the group G.

In this way Theorem 32 follows from remark C) of §31.

Proof of Theorem 33. Since we have now established Theorem 32 for all locally compact groups, Theorem 33 follows from remark E) of §31.

Proof of Theorem 35. Since Theorem 32 is now proved for all locally compact groups, Theorem 35 follows from remark F) of §31.

Hence all the results in the theory of characters which we formulated in §31 are now proved for general locally compact commutative groups satisfying the second axiom of countability.

The following natural question arises here: How can we explain the exceptional role played by the group K in the exposition of this theory, and is this choice of the group K accidental or not? The following proposition gives an answer to this question.

G) Let Q be a locally compact commutative group. We denote by $\overline{K}$ the group of all homomorphisms of the group K, and by $\overline{\overline{K}}$ the group of all homomorphisms of the group $\overline{K}$, in the group Q. Then the groups K and $\overline{\overline{K}}$ are isomorphic if and only if the group Q is isomorphic with the group K. Hence the group K is the only group which can be employed in the foundation of the theory of characters in order that the fundamental Theorem 32 should hold.

We now proceed to prove this. If $\overline{K}$ contains only zero, then $\overline{\overline{K}}$ also contains only zero, which contradicts the supposed isomorphism between the groups K and $\overline{\overline{K}}$. Hence there exists a non-zero homomorphism α of the group K into the group Q. Under this homomorphism α the group K maps into some subgroup K' of the group Q. Since the homomorphism α is not zero, the group K' is isomorphic with K (see §32, A)); while the homomorphism α itself is not necessarily an isomorphism. Hence Q contains a subgroup K' isomorphic with the group K.

We denote by P the maximal compact subgroup of the component of zero of the group Q (see §35, C)). Then $K' \subset P$. We shall prove that P decomposes into the direct sum of the subgroup K' and some subgroup L'.

We denote by G the character group of the group P, and suppose that $H = (G, K')$. Then G/H is the character group of the group K', i.e., G/H is a free cyclic group (see §32, F)). We denote by z one of the inverse images of a generator of the group G/H in the group G, and by Z the free cyclic subgroup of the group G having z as generator. It can readily be seen that G decomposes into the direct sum of the subgroups Z and H. Let $L' = (P, Z)$. Then P decomposes into the direct sum of the subgroups K' and L' (see Theorem 37 and 39). Every homomorphism β of the group K in the group Q maps K into P, $\beta(K) \subset P$, and since the group P decomposes into the direct sum of the subgroups K' and L', the group $\overline{K}$ of all homomorphisms decomposes into the direct sum of the subgroups A and B, where A is composed of all the homomorphisms of the group K in the group K', and B of all the homomorphisms of the group K in the group L'. Hence A is a free cyclic group, while the nature of the group B does not concern us.

Since the group $\bar{K}$ is decomposable into the direct sum of its subgroups A and B, the group $\bar{\bar{K}}$ of all the homomorphisms of the group $\bar{K}$ in the group Q decomposes into the direct sum of the subgroups C and D, where C is isomorphic to the group of all homomorphisms of the group A in the group Q, and D is isomorphic with the group of all homomorphisms of the group B in the group Q.

Since A is a free cyclic group, the group of all homomorphisms of the group A in the group Q is obviously isomorphic with the group Q itself. Hence the group C is isomorphic with Q.

The group $\bar{\bar{K}}$ is by assumption isomorphic with the group K. Therefore Q is isomorphic with some subgroup of the group K. Since, moreover, Q contains a subgroup K' isomorphic with K, it follows that the group Q is isomorphic with K.

This proves proposition G).

Proposition G) shows that the group K is actually exceptional, and is the only group which could have been used for the purpose of constructing the theory of characters. This peculiarity of the group K is emphasized by the fact that all factor groups of K contain either only zero, or else are isomorphic with the group K itself. This same property is possessed by finite groups of prime order, but these groups, being finite, cannot be used for the construction of the theory of characters.

Example 52. Let G be a locally compact group and X its character group. By Theorem 41 the component G' of zero of the group G decomposes into the direct sum of a vector group A and a compact group. In the same way the component X' of zero of the group X decomposes into the direct sum of a vector group Π and a compact group. Let $H = (G, \Pi)$. Making use of Theorems 32 and 33 we can show that G decomposes into the direct sum of the subgroups H and A, where H has a compact component of zero. Hence every locally compact group G can be decomposed into the direct sum of a vector subgroup A and a subgroup H having a compact component of zero.

We leave the proof of this proposition to the reader.

We shall call an element of the group G *compact* if all of its multiples are contained in a compact subset of the group G. The totality of all compact elements of the group G forms a group $(G, X') = Z$ such that the factor group G/Z contains no compact elements, and is decomposable into the direct sum of a vector group and a discrete group having no elements of finite order.

If the group G is a 0-dimensional group, then its character group contains only compact elements. Conversely, if the group G contains only compact elements, then its character group is a 0-dimensional group.

We leave the proofs of these propositions to the reader.

36. Locally Connected Commutative Groups

We shall occupy ourselves here with the investigation of locally compact commutative groups satisfying the rather special topological condition of being locally connected. This enables us, in particular, to clarify in greater detail

the structure of general locally compact commutative groups. The study of locally connected groups is of interest because it enables us to solve for commutative groups the so-called fifth problem of Hilbert, the problem of determining the structure of topological groups having a neighborhood which is homeomorphic with an open set of Euclidean space. The condition of being locally Euclidean can be applied to topological groups only with extreme difficulty, and we therefore replace it by another and weaker condition of local connectedness.

A) A topological space R is called *locally connected* if for every point $a \varepsilon R$ and neighborhood U of a there exists a neighborhood V of a such that for any $x \varepsilon V$ there exists a connected set $S \subset U$ which contains the points a and x.

A topological group is called *locally connected* if its topological space is locally connected.

Obviously every open set of Euclidean space satisfies the condition of local connectedness.

B) Let G and G^* be two topological spaces and f an open continuous mapping of the space G on the space G^* (see §18, C)). If the space G is locally connected, then G^* is also locally connected.

Let a^* be a point of G^*, and U^* a neighborhood of a^*. We denote by a a point of G such that $f(a) = a^*$, and by U a neighborhood of a for which $f(U) \subset U^*$. Furthermore, let V be a neighborhood of the point a, such that for $x \varepsilon V$ there exists a connected set $S \subset U$ containing the points a and x. Suppose that $V^* = f(V)$. Since the mapping f is open, V^* is open in G^*. For every point $x^* \varepsilon V^*$ there exists a point $x \varepsilon V$ such that $f(x) = x^*$. If now $S \subset U$ is a connected set containing a and x, then $S^* = f(S) \subset U^*$ is a connected set (see §11, E)), containing a^* and x^*. Hence G^* is locally connected.

We consider first of all the local topological structure of some groups of special form.

C) Let G be a discrete commutative group of finite rank r (see §6, A)) having no elements of finite order, and let X be the character group of the group G. Then there exists a neighborhood V of zero of the group X which is homeomorphic to the topological product of the spaces E and Φ (see Definition 21), where E is the interior of an r-dimensional cube, and Φ can be one of two things: a) Φ contains only one point, and then the group G admits a finite system of linearly independent generators, b) Φ is an infinite compact 0-dimensional group, in which case G does not have a finite system of generators.

Let

$$(1) \qquad a_1, \cdots, a_r$$

be a system of r linearly independent elements of the group G. We consider the neighborhood V' of zero of the group X which is defined by the compact set F composed of the points of the system (1), and by a neighborhood U of zero of the group K (see Definition 34) which consists of all elements a of the group K which satisfy the inequality $|a| < \frac{1}{4}$ (see §30, A)).

Every element x of the group G can be represented uniquely in the form

(2) $$x = s_1 a_1 + \cdots + s_r a_r,$$

where s_i, $i = 1, \cdots, r$, are rational numbers. Let

(3) $$d_1, \cdots, d_r$$

be a system of real numbers satisfying the inequalities

(4) $$|d_i| < \tfrac{1}{3}, \qquad i = 1, \cdots, r.$$

We associate with every system of numbers (3) a character

(5) $$\alpha(d_1, \cdots, d_r) = \alpha$$

of the group G. If $x \varepsilon G$ is defined by relations (2), then α is defined by letting

$$\alpha(x) = s_1 d_1 + \cdots + s_r d_r,$$

where the right member is considered as an element of the group K, i.e., is reduced modulo 1 (see §30, A)). The set of all characters of the form (5) will be denoted by E. Obviously E is homeomorphic to the interior of an r-dimensional cube. It follows from (4) that $E \subset V'$. The inverse relation, however, holds only in exceptional cases.

We denote by H the subgroup of the group G generated by elements of the system (1). Let $\Phi' = (X, H)$; then $\Phi' \subset V'$. Let γ be any character of the set V'. Then $\gamma(a_i) = d_i$, $i = 1, \cdots, r$, where $|d_i| < \frac{1}{3}$ since $\gamma \varepsilon V'$. Here the d_i are considered simply as real numbers. Let $\alpha = \alpha(d_1, \cdots, d_r)$ (see (5)); then $\beta = \gamma - \alpha \varepsilon \Phi'$, since the characters γ and α coincide on the subgroup H. In this way every element $\gamma \varepsilon V'$ is represented in the form $\gamma = \alpha + \beta$, where $\alpha \varepsilon E$, $\beta \varepsilon \Phi'$. It is not hard to see that this representation is unique. Therefore the neighborhood V' decomposes into the direct sum of the set E and the subgroup Φ'. From this it follows that V' is homeomorphic to the topological product of the set E and the set Φ'.

We now make clear the structure of the set Φ'. By Theorem 34, Φ' is the character group of the group $G^* = G/H$. If the group G^* is finite, Φ' contains only a finite number of elements. Then E is an open set in V' and therefore E is a neighborhood of zero of the group X. We have here case a). Since H has a finite system of generators, and since G^* is finite, it follows that G also admits a finite system of generators; and since G has no elements of finite order, it must admit a finite system of linearly independent generators (see §6, F)). If the group G^* is infinite, we denote by $H_1^*, \cdots, H_n^*, \cdots$ an infinite increasing sequence of finite subgroups of the group G^*, whose sum coincides with G^*. Such a sequence exists in G^* since every element of G^*, as can easily be seen, is of finite order. Let $\Phi_n' = (\Phi', H_n^*)$. Then the intersection of all the groups of the decreasing sequence $\Phi_1', \cdots, \Phi_n', \cdots$ contains only zero, and therefore there exist arbitrarily small groups in this sequence. On the other hand, the factor group Φ'/Φ_n', being the character group of the group H_n^*, is

finite. Hence the group Φ' has arbitrarily small open subgroups, and therefore Φ' is a 0-dimensional group (see §22, G)). At the same time Φ' is infinite since G^* is infinite. We have here case b). The group G does not admit a finite system of generators, for were such a system to exist in G, it would also exist in the factor group G^*. But then G^* would be finite since all of its elements are of finite order.

Hence C) is proved.

D) Let G be a discrete commutative group of finite rank r (see §6, A)) having no elements of finite order. The character group X of the group G is locally connected if and only if the group G admits a finite system of linearly independent generators.

The proof of D) follows directly from C). Case a) gives a locally connected group, while in case b) local connectedness is obviously impossible, since every neighborhood V splits up into separate slabs converging to each other.

In order to consider infinite ranks we prove the following proposition.

E) Let G be a discrete group having no elements of finite order. If every increasing sequence $H_1, \cdots, H_n, \cdots$ of subgroups of a constant finite rank r becomes constant after a certain n, then the group G decomposes into the direct sum of a finite or infinite number of infinite cyclic subgroups.

To prove this we shall construct by induction the sequence

$$G_0, G_1, \cdots, G_r, \cdots \tag{6}$$

of subgroups of the group G, which comprises the whole group G, and is such that the following conditions are satisfied: a) the subgroup G_r is the maximal subgroup of the group G having the rank r; this is to be understood in the sense that every subgroup H of rank r which contains G_r coincides with G_r, b) the subgroup G_r admits a finite system of linearly independent generators

$$a_1, \cdots, a_r, \tag{7}$$

c) the system of linearly independent generators for G_{r+1} is obtained by adjoining to the system (7) the single element a_{r+1}.

We number the set of all elements of the group G by denoting them by

$$g_1, \cdots, g_n, \cdots. \tag{7'}$$

We construct the sequence (6) by induction. We take for G_0 the subgroup which contains only zero. Let us suppose that the subgroup G_r has already been constructed. If the rank of the group G is r, then by a), $G = G_r$, and hence G admits a finite system of linearly independent generators (see b)), i.e., it decomposes into the direct sum of a finite number of infinite cyclic subgroups (see §6, F)). If the rank of the group G exceeds r, then the sequence (7′) contains elements not belonging to G_r; we denote the first such element by x_r. By adjoining to the group G_r the element x_r we obtain a subgroup H_1 of rank $r + 1$ which contains G_r and has a finite number of generators. If H_1 is not the maxi-

mal group of rank $r + 1$ we can adjoin to H_1 an element of the group G in such a way that the resulting group H_2 will contain H_1 but will preserve the rank $r + 1$. Continuing this process, we obtain an increasing sequence of subgroups of rank $r + 1$, each of which admits a finite system of generators. This sequence after a finite number of steps becomes constant on reaching a maximal group of rank $r + 1$ with a finite number of generators. We shall denote this group by G_{r+1}. Let (7) be the system of linearly independent generators of the group G_r. We shall show that we can obtain from it the system of generators for the group G_{r+1} by adjoining one element to the system (7). Let $G^* = G_{r+1}/G_r$. The group G^* admits a finite system of generators since the group G_{r+1} admits such a system. Furthermore, G^* has no elements of finite order. In fact, if H^* is the subgroup of the group G^* composed of all elements of finite order, then we denote by H the complete inverse image of the group H^* in the group G_{r+1}. Then it can easily be seen that H is a group of rank r which contains the group G_r, and therefore by condition a), $H = G_r$, which means that H^* contains only zero. Therefore the group G^*, being of rank 1 as can readily be seen, is an infinite cyclic group having a generator a^* (see §6, F)). We denote one of the inverse images of the element a^* in the group G_{r+1} by a_{r+1}. It is obvious that the system $a_1, \cdots, a_r, a_{r+1}$ is a system of linearly independent generators of the group G_{r+1}.

This completes the induction.

If the construction of the sequence (6) terminates after a finite number of steps, then the group G decomposes into a finite direct sum of infinite cyclic subgroups. If the sequence (6) is continued indefinitely then we denote by

$$a_1, \cdots, a_r, \cdots \tag{8}$$

an increasing sequence of linearly independent generators of the groups of the sequence (6) (see b) and c)). Then the system (8) gives an infinite sequence of linearly independent generators of the group G. If we denote by A_i an infinite cyclic group having the generator a_i, then it is not hard to see that G decomposes into the direct sum of the subgroups $A_1, \cdots, A_r, \cdots$. Hence proposition E) is proved.

THEOREM 42. *A compact locally connected and connected commutative group X decomposes into the direct sum of a finite or countable number of subgroups, each isomorphic with the group K* (see §30, A)).

PROOF. Let G be the character group of the group X. Then by Theorem 32, X is the character group of the group G, where G is discrete (see Theorem 31). Since the group X is connected, the group G has no elements of finite order (see Example 48). Suppose that the group G does not satisfy the conditions of remark E), i.e., that G contains an unlimited expanding sequence of subgroups

$$H_1, \cdots, H_n, \cdots \tag{9}$$

of a constant finite rank r. We denote by H the minimal subgroup containing all the subgroups H_n. Since the sequence (9) expands without limit, the group H cannot admit a finite system of generators. Let $\Phi = (X, H)$. Then $X^* = X/\Phi$ is the character group of the group H (see §32, M)). Since the group X is locally connected, the factor group X^* is also locally connected (see B)). But then by remark D) the group H admits a finite system of generators, and therefore we have arrived at a contradiction. Therefore the group G satisfies the conditions of remark E) and it follows that X decomposes into the direct sum of a finite or infinite number of subgroups isomorphic with the group K (see Theorem 39 and §32, F)). Hence Theorem 42 is proved.

Theorem 42 can easily be generalized to non-connected groups.

F) A compact locally connected commutative group X can be decomposed into the direct sum of a finite or infinite number of groups isomorphic with K, and a finite group.

We denote by X' the component of zero of the group X. From the local compactness of the group X follows the local compactness of the groups X' and X/X' (see B)). The group X/X' is 0-dimensional and compact, and therefore, being locally connected, must be finite. For were X/X' infinite, it would have zero for a limit element, i.e., there would exist some element a in every neighborhood of zero. But zero and a cannot both be included in a connected set, since X/X' is a 0-dimensional group. Therefore the supposition that X/X' is infinite contradicts the assumption of local connectedness. The The group X' is connected and by Theorem 42 decomposes into the direct sum of a finite or countable number of groups isomorphic with K. From the facts that X' has such a simple structure and that the factor group X/X' is finite it follows easily that X is decomposable into the direct sum of the group X' and a finite group.

THEOREM 43. *A locally compact locally connected and connected commutative group G decomposes into the direct sum of a finite number of groups isomorphic with the additive group of real numbers and a finite or countable number of groups isomorphic with the group K* (see §30, A)).

PROOF. By Theorem 41, the group G decomposes into the direct sum of a vector group A and a compact group Z. Since G is connected Z is also connected (see §11, E)). Furthermore, since G is locally connected its factor group $G/A = Z$ is also locally connected (see B)). Hence by Theorem 42, Z decomposes into the direct sum of a finite number of groups isomorphic with K. The vector group A in turn decomposes into a direct sum of a finite number of groups, isomorphic with the group of real numbers. Hence Theorem 43 is proved.

THEOREM 44. *If a locally compact commutative group G has a neighborhood of zero homeomorphic to an open set of Euclidean space, then it decomposes into the direct sum of a finite number of groups isomorphic with the group of real numbers, and a finite number of groups isomorphic with the group K* (see §30, A)).

PROOF. It follows from the fact that G has a neighborhood of zero homeomorphic to an open set of Euclidean space that G is locally connected, and therefore satisfies the conditions of Theorem 43. However, it would be impossible here to have an infinite number of direct summands isomorphic with the group K, since in that case the group G would have infinitely many dimensions. This proves the theorem.

EXAMPLE 53. Let G' be the discrete additive group of rational numbers, and G one of its subgroups distinct from zero, Obviously G has no elements of finite order and its rank is equal to 1. Therefore the character group X of the group G is connected and one-dimensional (see Examples 48 and 49).

It is not hard to see that every compact connected group of dimensionality 1 can be obtained as the character group of a group $G \subset G'$. If the group G has a finite system of generators, then it is an infinite cyclic group. Hence since the group X is locally connected, it is isomorphic with the group K (see D) and §32, F)).

The group X considered here has been investigated in detail by van Dantzig [8], who called these groups *solenoidal groups.*

It has been supposed that every finite-dimensional connected compact group decomposes into the direct sum of solenoidal groups. This supposition has, however, been shown to be false. In fact there exists a two-dimensional connected compact group which in general does not decompose into a direct sum. The construction of this example can be achieved by constructing a discrete group G of rank 2 having no elements of finite order which does not decompose into a direct sum. Then the character group of the group G gives the desired example of a compact topological group (see [28]).

37. Topologized Algebraic Fields

It is natural to consider together with topological groups some other topologized algebraic structures. We meet very frequently in mathematics with just such structures; it is sufficient to point out the field of real numbers, and the field of complex numbers. These fields are not purely algebraic structures, since limiting processes play in them as important a part as the operations of addition and multiplication. The question of the structure of topologized algebraic fields seems to me of interest because its solution would clarify the role played by real and complex numbers and give a reason for their exceptional position in mathematics. What is it that separates them from other analogous entities? Real and complex numbers arise in mathematics in a purely constructive way. It is desirable now to give a deductive definition for them, and to show that their exceptional position is not due to historic accident, but is a necessity arising from very general considerations.

The above investigation of topological groups makes the solution of this problem almost trivial.

DEFINITION 37. A set K is called an *algebraic field*, or simply a *field*, if two operations are established in K: *addition* and *multiplication*, which satisfy the

following conditions: The set K forms a commutative group under the operation of addition. The zero of this group is called the *zero* of the field K. Under multiplication the totality of all the elements of the set K with the exception of zero also forms a group, in general not commutative. The identity of this group is called the *identity* of the field K. By definition the product of zero by an arbitrary element is equal to zero. The operations of addition and multiplication are connected by *distributivity* conditions

$$x(y + z) = xy + xz, \qquad (y + z)x = yx + zx.$$

A field K is called *topological* if the set K is a topological space, and if the algebraic operations operating in K are continuous in the topological space K.

Well-known examples of topological fields are the fields of the real and complex numbers with their natural topologies and the usual operations of addition and multiplication. Both these fields are commutative. An example of a non-commutative topological field is afforded by quaternions.

A) Let us denote by K_2 the set of all linear forms of the type

$$a + bi + cj + dk = x, \tag{1}$$

where a, b, c, d are real numbers, while the symbols i, j, k are as yet undefined. Addition can be defined naturally in the set K_2 as the addition of linear forms. We shall now define the operation of multiplication in the set K_2. We shall agree beforehand that multiplication is to be distributive and associative, that real numbers are to be multiplied in the usual manner, and that they commute with all quantities. Under these conditions in order to define the law of multiplication it is sufficient to define the product of the *quaternion units* i, j, k. We set

$$i^2 = -1, j^2 = -1, k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j. \tag{2}$$

A topology can be introduced naturally into the set K_2, and the resulting topological field is called the *field of quaternions*, and its elements are called *quaternions*.

The *norm* of the quaternion x (see (1)) is the nonnegative real number

$$|x| = +\sqrt{[a^2 + b^2 + c^2 + d^2]}. \tag{3}$$

Direct calculation shows that if x and y are two quaternions, then

$$|xy| = |x||y|, \tag{4}$$

and

$$|x + y| \leqq |x| + |y|. \tag{5}$$

The inverse of the quaternion x is the quaternion x^{-1} defined by

$$x^{-1} = |x|^{-2}(a - bi - cj - dk). \tag{6}$$

In this way every quaternion whose norm is different from zero has an inverse, and the norm zero corresponds to the quaternion zero.

It is not necessary for our purposes to go into greater detail about the properties of quaternions.

We can define in a natural way isomorphism between topological fields. Two topological fields K' and K are said to be *isomorphic* if there exists a homeomorphic mapping of the field K on the field K' which preserves the operations of addition and multiplication.

THEOREM 45. *Let K be a locally compact connected topological field satisfying the second axiom of countability. Then K is isomorphic with one of three topological fields D, K_1, K_2, where D is the field of real numbers, K_1 is the field of complex numbers, and K_2 is the field of quaternions.*

As a preamble to the proof of this theorem we make the following remark.

B) A topological field K satisfying the conditions of Theorem 45 contains a subfield D isomorphic with the field of real numbers, and such that every element of D commutes with every element of K. Furthermore K contains a finite system of elements $x_1, \cdots, x_r$, such that every element x of the field K can be naturally represented in the form

$$x = a_0 + a_1x_1 + \cdots + a_rx_r$$

where $a_i \varepsilon D$, $i = 0, 1, \cdots, r$.

Let us show first of all that K cannot be compact. K contains at least two elements, zero and one. Therefore, being connected, the field K must have zero for a limit element. Let $y_1, \cdots, y_n, \cdots$ be a sequence of elements of the field K which are distinct from zero, but converge to zero. Then the sequence of inverse elements $y_1^{-1}, \cdots, y_n^{-1}, \cdots$ cannot have a limit element. Therefore the field K is not compact.

Since K is a commutative group under addition, it follows from Theorem 41 that this group is decomposable into the direct sum of a vector group A and a compact group Z. Let a be an element of the subgroup A distinct from zero. Then the sequence

$$a, 2a, \cdots, na, \cdots \tag{7}$$

of integral multiples of the element a has no limit points in K. Furthermore let z be an element of the group Z distinct from zero. The sequence

$$z, 2z, \cdots, nz, \cdots \tag{8}$$

of integral multiples of the element z has limit points in K since Z is compact. But the sequence (8) can be obtained from the sequence (7) by multiplication by $a^{-1}z$ and hence, because of the continuity of the operation of multiplication, the sequences (7) and (8) simultaneously do or do not have limit elements. Therefore, the assumption that both subgroups A and Z contained elements distinct from zero leads to a contradiction, and hence one of the subgroups

must contain only zero. And since K is not compact, Z must contain only zero, and K coincides with A.

Hence K, being an additive group, is isomorphic with a vector group. We shall think of K simply as an additive vector group.

The product ax of a vector x by a real number a is defined in K. We denote by e the identity of the field K and show that

$$(bx)(ae) = (ab)x \tag{9}$$

and

$$(ae)(bx) = (ab)x \tag{10}$$

where a and b are all real numbers and $x \varepsilon K$.

Relation (10) is obvious when a is a positive integer n, for then $ne = e + \cdots + e$, and (10) follows from the distributivity of multiplication in K. If n is a negative integer, we can easily show (10) to be true for n by letting $n' = -n$. It follows in this way for an integer $n \neq 0$ that $(ne)(1/n)e) = e$, i.e., $(ne)^{-1} = (1/n)e$. Furthermore, for $n \neq 0$ we have $(nb)x = (ne)(bx)$. Multiplying both sides of this relation by $(ne)^{-1}$ we get $((1/n)e)(nbx) = ((1/n)nb)x$. Letting $nb = c$ we get $((1/n)e)(cx) = ((1/n)c)x$. Hence (10) is proved for $a = 1/n$. Let now m and $n > 0$ be integers. From what we have just shown $((m/n)e) = (me)((1/n)e)$. Multiplying this by bx we get $((m/n)e)(bx) = (me)((1/n)e)(bx) = (me)((b/n)x) = ((m/n)b)x$. Hence (10) is proved for a rational a. Because of the continuity of the operation of multiplication in K, we can now extend relation (10) to an arbitrary real number a.

Relation (9) is proved in like manner.

We denote by D the set of all the elements of the field K which can be written in the form de, where d is a real number, and e is the identity of the field K. If a and b are two real numbers, then it follows from the properties of the vector space K that $ae + be = (a + b)e$. Moreover, it follows from (10) that $(ae)(be) = (ab)e$. This shows that the set D is a field isomorphic with the field of real numbers. Relations (9) and (10) taken together show that every element of the set D commutes with every element of the field K.

We now select in K a complete system of linearly independent vectors, which include the vector e. Let $e, x_1, \cdots, x_r$ be this system. Then every element x of the vector space K can be written uniquely in the form

$$x = b_0 e + b_1 x_1 + \cdots + b_r x_r$$

where b_i, $i = 0, 1, \cdots, r$, real numbers. But by (10) this same element x can also be written in the form

$$x = a_0 + a_1 x_1 + \cdots + a_r x_r$$

where $a_i \varepsilon D$, $i = 1, \cdots, r$.

Hence B) is proved.

Frobenius has shown that every field of the type to which we have reduced K is isomorphic with one of the fields D, K_1, or K_2. Hence Theorem 45 follows from this result of Frobenius, the proof of which follows.

PROOF OF THEOREM 45. We shall simply identify the field D constructed in remark B) with the field of real numbers.

a) if $K = D$, then Theorem 45 already holds for the field K.

b) We now denote by I the set of all elements $z \in K$ for which the following conditions are fulfilled; $z^2 \in D$, $z^2 \leqq 0$, and show that every element $x \in K$ can be decomposed uniquely into the sum.

$$x = d + z, \quad \text{where} \quad d \in D, \qquad z \in I. \tag{11}$$

Consider the sequence

$$1, x, x^2, \cdots, x^n, \cdots \tag{12}$$

of powers of an element x. Since by remark B) the field K is a vector space of a finite number of dimensions, the elements of the sequence (12) are linearly dependent with respect to the field D of real numbers. Therefore there exists a polynomial $f(y)$ with real coefficients which reduces to zero when the unknown y is replaced by the element x, $f(x) = 0$. We can assume that $f(y)$ is irreducible; and it is well known that an irreducible polynomial in the domain of real coefficients is of the first or second degree. If $f(y) = y - d$, then $x = d \in D$, and the decomposition (11) is established. Let now $f(y) = y^2 + py + q$. By a simple algebraic transformation the polynomial $f(y)$ can be reduced to the form $f(y) = (y - d)^2 + c^2$. Let $x - d = z$: then $z \in I$ and hence $x = d + z$.

Hence (11) is proved. Suppose that we have also $x = d' + z'$, where $d' \in D, z' \in I$. Then $z' = z + d - d'$. Squaring both sides of this relation we get $z'^2 = z^2 + (d - d')^2 + 2(d - d')z$, from which it follows that $(d - d')z$ is a real number. But this is possible only if $d - d' = 0$ or $z = 0$. In either case the uniqueness of the decomposition (11) readily follows.

c) We shall now show that I is a linear subset of elements of K, i.e.,

$$ax + by \in I, \tag{13}$$

if $x \in I$, $y \in I$, and a and b are real numbers.

We shall first consider the case where x, y, and 1 are linearly dependent with respect to the field D of real numbers, i.e., where there exist real numbers α, β, γ not all zero such that $\alpha x = \beta y + \gamma$. It can readily be seen that the elements αx and βy belong to I, and therefore because of the uniqueness of the decomposition (11), $\gamma = 0$. Hence $y = (\alpha/\beta)x$ and the element $ax + by$ assumes the form $(a + b(\alpha/\beta))x$, from which (13) follows directly.

Let us now suppose that the element $ax + by$ can belong to D only under the condition $a = 0$, $b = 0$. Let

$$ax + by = d' + z' \tag{14}$$

where $d' \varepsilon D$, $z' \varepsilon I$ (see (11)). Here the elements d' and z' depend on the choice of the real numbers a and b; z' reduces to zero if and only if $a = b = 0$. We must show that $d' = 0$ for an arbitrary choice of a and b. Let

$$(15) \qquad xy + yx = d + z$$

(see (11)). Squaring both sides of (14) we get

$$(16) \qquad \begin{aligned} d'^2 + z'^2 + 2d'z' &= a^2x^2 + b^2y^2 + ab(xy + yx) \\ &= a^2x^2 + b^2y^2 + abd + abz. \end{aligned}$$

Since the decomposition (11) is unique it follows from (16) that

$$(17) \qquad 2d'z' = abz.$$

Suppose that d' is not equal to zero for at least one pair of values a, b. Then equation (17) shows that $z \neq 0$, and this means in turn that $d' \neq 0$ if $ab \neq 0$ since z does not depend on the choice of a and b. Hence we have

$$(18) \qquad z' = \frac{ab}{2d'} z,$$

where the equation always has a meaning when $ab \neq 0$. Hence

$$(19) \qquad ax + by = \frac{ab}{2d'} z + d'.$$

Since z does not depend on the numbers a and b and since equation (19) has a meaning whenever $ab \neq 0$, it follows that (19) can give two independent relations connecting the elements x, y, and z. Eliminating z from them we get $a'x + b'y = c'$, which contradicts the original relation. Hence we have arrived at a contradiction by supposing that d' is distinct from zero for some pair of values a and b. This means that $d' = 0$, and hence the linearity of the set I is established.

d) Let i and j be two elements of K such that $i^2 = -1$, $j^2 = -1$, and $k = ij \varepsilon I$. We shall show that the elements i, j, and k are linearly independent with respect to the field D and form a system of quaternion units, i.e., they satisfy relation (2).

Since $ij \varepsilon I$, we can write ij in the form al, where $a \varepsilon D$ and $l^2 = -1$. We have $(ij)(ji) = i(-1)i = 1$. Hence $ji = (al)^{-1}$. The element $(al)^{-1}$ can easily be seen to be equal to $-a^{-1}l$, and hence $ji = -a^{-1}l$. Since I is a linear set, and since the elements i and j belong to I, it follows that $i + j \varepsilon I$. Hence $(i + j)^2 = i^2 + j^2 + ij + ji$ is a real number, and this means that $ij + ji$ is also a real number. It follows from this that $(a - (1/a))l \varepsilon D$, i.e., $a^2 = 1$, and hence the condition $k^2 = -1$ is satisfied for $k = al$. We have therefore

$$(20) \qquad i^2 = -1, \qquad j^2 = -1, \qquad k^2 = -1.$$

Taking inverses on both sides of the equation

(21) $$ij = k$$

we get $j^{-1}i^{-1} = k^{-1}$, or what is the same (see (20)), $ji = -k$. Multiplying relation (21) on the left by $-i$ we get $j = -ik$. The remaining relations of the system (2) are obtained in the same manner. We now suppose that the relation

(22) $$bi + cj + dk = 0$$

holds with real coefficients. Multiplying (22) on the left by k we get $bj = ci + d$. Because of the uniqueness of (11) we have $d = 0$, and this means that $bij = -c$, which is possible only when $b = c = 0$, since $(ij)^2 = -1$. This proves the linear independence of the elements i, j, and k.

e) Let us suppose that $K \neq D$, but that any two elements in I are linearly dependent with respect to the field D. Then the field K is isomorphic with the field K_1 of complex numbers. In fact, let us select an element i in I such that $i^2 = -1$. Since any two elements in the set I are linearly dependent, it follows from the decomposition (11) that every element of K can be uniquely represented in the form $a + bi$ where a and b are real numbers, and this means that K is isomorphic with the field of complex numbers.

f) Suppose now that I contains two elements x and y, linearly independent with respect to the field D. We can then show that K contains a subfield K_2 isomorphic with the field of quaternions.

Let $xy = z + d$, where $z \varepsilon I$, $d \varepsilon D$ (see (11)). Then we can select a real number a such that $ax^2 = -d$, and for this particular number a we would have $x(u + ax) = z$. Since x and y are linearly independent, $x \neq 0$ and $y' = y + ax \neq 0$, where $y' \varepsilon I$ since I is a linear set (see c)). Normalizing x and $y' = y + ax$ by real multipliers we get elements i and j such that $i^2 = -1$, $j^2 = -1$, $ij = k \varepsilon I$. Then the elements i, j, and k are linearly independent and satisfy the relations of quaternion units (see d)). It can be seen readily that the set of all linear forms $a + bi + cj + dk$ forms a subfield K_2 of the field K which is isomorphic with the field of quaternions.

g) Suppose finally that the field K contains the subfield K_2 of quaternions. We then show that in this case $K = K_2$.

Let i, j, and k be the quaternion units of the field K_2. If the field K contains some elements not belonging to K_2, then we can find an element $z \varepsilon I$ which is linearly independent of the units i, j, k. Let

$$iz = d_1 + z_1, \qquad jz = d_2 + z_2, \qquad kz = d_3 + z_3$$

(see (11)). Suppose further that

$$l = a(z + d_1i + d_2j + d_3k),$$

where a is a real number. Then since I is linear (see c)), $il \varepsilon I$, $jl \varepsilon I$ and $kl \varepsilon I$. Furthermore, since I is a linear system and since z is linearly independent of the units i, j, k, we can select the number a in such a way that $l^2 = -1$. Then

the elements i, l, and il form a system of quaternion units (see c)). In particular $il = -li$, $(il)^2 = -1$. The same is true for the elements j and k, and we get

$$(23) \qquad (il)^2 = (jl)^2 = (kl)^2 = -1, \quad il = -li, \quad jl = -lj, \quad kl = -lk.$$

It follows from relation (23) that on one hand

$$(24) \qquad (il)k = (-li)k = l(-ik) = lj,$$

while on the other

$$(25) \qquad (il)k = i(lk) = i(-kl) = (-ik)l = jl.$$

Equations (23), (24), and (25) give $2jl = 0$, which contradicts the relation $(jl)^2 = -1$. Hence we have arrived at a contradiction, assuming that $K \neq K_2$.

This proves Theorem 45.

Example 54. Let K be the field of rational numbers. We introduce a topology into K by assigning a system of neighborhoods of zero in the field K as follows: Every rational number $r \varepsilon K$ can be written in the form $p^k(m/n)$, where p is a prime number fixed for a given construction, m and n are integers not divisible by p, and k may be positive or negative or zero. A neighborhood U_s of zero in the field K is defined as the totality of all numbers r for which $k \geqq s$, where s is a positive integer. Hence the higher the power of p by which r is divisble, the closer is the element r to zero. The topological field thus obtained will not be locally compact, but it can be made so through addition of new elements which are sequences of elements of the field K, just as is done in introducing real numbers. This enlarged locally compact field K is called the field of p-adic numbers. It is not connected.

CHAPTER VI

THE CONCEPT OF A LIE GROUP

So far, in considering topological groups, we have imposed upon them conditions of a rather general character formulated in terms of abstract algebra and abstract topology. The concept of a Lie group, however, contains in its very definition the condition of analyticity—or at least of differentiability—of the functions which define the operation of multiplication in the group (see Definition 38). Therefore in studying Lie groups we can avail ourselves of the machinery of analysis, including the theory of integration of differential equations. Because of these possibilities Lie groups admit a very detailed investigation which finally reduces their study to that of some elementary, although very delicate algebraic problems. These problems are essentially some special problems in the theory of matrices. Only after these considerations begins the really refined and deep theory of Lie groups. However, we shall not take up these problems in the present chapter.

Usually in theories of an older date the question of the differentiability or analyticity of the functions under consideration was not subjected to a rigorous scrutiny. All the functions arising in the consideration of certain given functions were simply assumed when necessary to be differentiable or analytic. This, however, has one serious defect. It is one thing to suppose that some definite functions appearing in the definition of a given object are differentiable, and quite another thing to suppose in advance the differentiability of all functions which may arise in the process of investigation of this object. In actual fact we may know nothing in advance of the nature of these functions; we cannot compute them *a priori* and it may happen that a thoroughly natural problem leads to non-differentiable functions. This is precisely the unsatisfactory situation in the classical theory of Lie groups. Let us suppose for example that we are investigating a given Lie group G. Although it does not follow *a priori* that every subgroup of this Lie group is also a Lie group, still the necessity of considering such subgroups may easily arise. The same is true in connection with factor groups. It may also become necessary to discuss the automorphisms of a Lie group. Can they be expressed in terms of differentiable functions? We devote this chapter to the solution of these preliminary questions. Starting with the differentiability or analyticity of some definite functions we arrive at the differentiability or analyticity of a series of functions which arise naturally in the course of the investigation. It would in fact be possible to limit ourselves to the single assumption of differentiability, since with this assumption we can reduce our entire investigation, without loss of generality, to that of analytic functions. We shall be forced, however, to make a double investigation in this chapter, assuming differentiability and analyticity in turn, as the corresponding proof of the reduction of differentiable to analytic func-

tions is beyond the scope of the present chapter. On the other hand we cannot limit ourselves to differentiable functions alone, for in that case the results of the following chapter will not be complete.

If, however, the reader is willing to confine himself to the classical way of handling this problem and does not care to enter more deeply into the fundamental principles discussed above, he need not read this chapter in its entirety. It would then be sufficient to read §§38, 39, and 42, omitting Theorem 48.

In the classical theory a Lie group G is defined as any local group in which differentiable coordinates D have been introduced (see Definition 38). The properties of the group G are those properties of the system of equations (3) of §38 which remain invariant under a differentiable transformation of the coordinates D (see §38. A)). Furthermore by a subgroup H of the group G is understood only such a subgroup as is defined by relations (1) of §41, i.e. Theorem 50 is reduced to a definition. In the same way only those homomorphisms χ which are defined by relations (21) of §41 are admitted as homomorphisms of the group G, i.e. Theorem 51 is also reduced to a definition.

The results of this chapter are intended primarily as preparatory material for Chapter VII in which we shall show that the study of compact topological groups satisfying the second axiom of countability can be reduced to the study of Lie groups. There we shall also define compact Lie groups in general terms without making use of the concept of differentiability.

Because of the great many calculations which we shall have to face in this and the ninth chapter, we make use of tensor notation in both these chapters, without assuming, however, a knowledge of tensor calculus. We shall simply eliminate the summation sign $\sum$. The usual rule is that indices are written both as subscripts and as superscripts, and if a monomial has the same index i as both subscript and superscript then this monomial represents a sum over i, i going over all possible values. If a monomial contains not one double index but several, then this monomial represents a corresponding multiple sum. For example the monomial a_ib^i stands for $\sum_{i=1}^{r} a_ib^i$, while $c_{ij}^k a^j$ stands for the double sum $\sum_i\sum_j c_{ij}^k a^j$. It is not permissible to interchange the subscripts with the superscripts, so that every system of numbers has a definite distribution of indices. This distribution should of course be carried out in some convenient way. In particular, the coordinates of points and the components of vectors are denoted by letters with superscripts, where the letters chosen are the same as those used for the points and vectors themselves. For example the coordinates of the point x are denoted by $x^1, x^2, \cdots, x^r$. We shall not write the upper indices in parentheses to distinguish them from powers, but on the contrary when we want to raise a letter to some power we shall use parentheses as follows: $(a)^n$ will mean the n-th power of a. However powers will hardly be met with in our discussions. We shall denote by δ_j^i a number equal to unity for $i = j$ and equal to zero for $i \neq j$.

38. Lie Groups

The classical theory of Lie groups studies first of all local Lie groups, and therefore we shall give here the definition of a local Lie group, which however is applicable to entire groups.

DEFINITION 38. A local group G (see §23, D)) is called a *local Lie group*, if the following conditions are fulfilled:

1) A *coordinate system* can be introduced in G. This means that there exists a topological mapping φ of a neighborhood U of zero of the group G on an open set V of a Euclidean space S, under which the identity transforms into the origin. In this way to a point $x \varepsilon U$ corresponds a system of real numbers

$$(1) \qquad x^1, x^2, \cdots, x^r$$

which are the coordinates of the point $\varphi(x) \varepsilon S$. We shall call these numbers the *coordinates* of the point $x \varepsilon U$. The identity will have its coordinates equal to zero. Furthermore, to every system of numbers (1), if these numbers are sufficiently small in absolute value, corresponds a definite point $x \varepsilon U$ having these numbers for its coordinates. The dimension r of the space S is called the *dimension* of the group G.

Let W be a sufficiently small neighborhood of the identity of the group G, so that for any two elements x and y in W the product xy is defined and $xy \varepsilon U$. We then have

$$(2) \qquad xy = z = f(x, y).$$

Since all the points x, y, and z belong to U, they all have coordinates, and in coordinate form relation (2) can be rewritten as

$$(3) \qquad z^i = f^i(x, y) = f^i(x^1, \cdots, x^r; y^1, \cdots, y^r)$$

where the functions f^i in the right side of the equation are continuous functions defined for all sufficiently small values of the arguments. Since furthermore $xe = x$, $ey = y$, we have

$$(4) \qquad f^i(x^1, \cdots, x^r; 0, \cdots, 0) = x^i, \quad f^i(0, 0, \cdots, 0; y^1, \cdots, y^r) = y^i.$$

2) *Differentiable* coordinates can be introduced into G. More precisely, for some choice of a neighborhood U and a mapping φ, the functions f^i which appear in the right side of (3) have all their third derivatives, and these derivatives are continuous.

It follows from (4) that

$$(5) \qquad \frac{\partial f^i}{\partial x^j} = \frac{\partial f^i}{\partial y^j} = \delta_j^i \quad \text{for} \quad x = y = e,$$

where $\|\delta_j^i\|$ is the unit matrix.

3) *Analytic* coordinates can be introduced into G. This means that for some choice of a neighborhood U and a mapping φ, the functions appearing in the right side of (3) are analytic.

An entire topological group G is called a *Lie group* if it satisfies the second axiom of countability, and is a local Lie group i.e., if in some neighborhood of the identity coordinates can be introduced in the proper way.

It can readily be seen that a Lie group is always locally compact. Obviously condition 2) is a direct consequence of condition 3). In this chapter we shall distinguish between *analytic Lie groups*, i.e., Lie groups satisfying condition 3) and *differentiable Lie groups*, which satisfy condition 2). We shall show in the ninth chapter that analytic coordinates can be introduced into every differentiable Lie group. Hence the distinction which we have introduced here is temporary and conditional.

We shall formulate here one important problem, the so-called fifth problem of Hilbert. This problem can now be stated as follows: Is condition 3) a consequence of condition 1)? This has been answered in the affirmative for compact and for commutative groups (see Theorems 37 and 44). In the general case this still remains an open question.

The whole investigation of a Lie group G is built on the properties of the differentiable coordinates which can be introduced into it. We study not the properties of the group G itself, but the properties of the system (3) which expresses the law of multiplication in G. Actually we study only such properties of this system which do not depend on the choice of coordinates in G, and which therefore express properties of the group G itself. First of all it is clear that together with some definite system D of differentiable coordinates we can consider a whole set $[D]$ of coordinate system obtained from D by means of differentiable transformations (see A)). We should therefore endeavor to study only those properties of the system (3) which hold in all the coordinates of the totality $[D]$. Since this has to do with finding the invariants of the system (3) under differentiable transformations of coordinates, no particular difficulty arises at this point. We should further clarify the question of whether there exists in $[D]$ a differentiable system of coordinates D' such that a differentiable transition from the system D to the system D' is impossible. We shall show below (see §40) that such a system does not exist, and therefore that the whole question of finding all the properties of the group G reduces to the question of finding such properties of the system (3) which remain unaltered under differentiable transformations of coordinates.

We shall recall here the definition of a differentiable and of an analytic transformation of coordinates.

A) Let G be a local Lie group and D some definite differentiable or analytic system of coordinates in G (see Definition 38). The coordinates of a point x in the system D are denoted as usual by x^i. Let

$$\varphi^i(x) = \varphi^i(x^1, \cdots, x^r), \qquad i = 1, \cdots, r, \tag{6}$$

be a system of differentiable functions having three continuous derivatives, or a system of analytic functions, such that

$$\varphi^i(e) = \varphi^i(0, \cdots, 0) = 0. \tag{7}$$

Let

$$p_j^i = \frac{\partial \varphi^i(e)}{\partial x^j} \tag{8}$$

and suppose that the determinant of the matrix $\|p_j^i\|$ is different from zero. Then the system of equations

$$x'^i = \varphi^i(x^1, \cdots, x^r) \tag{9}$$

can be thought of as introducing a new system of coordinates in G, i.e., the new coordinates of the point x are the numbers x'^i. It can readily be seen that if both the original coordinates D and the transformation (9) are differentiable or analytic, then the new coordinates D' will be correspondingly differentiable or analytic.

B) Let G be a local Lie group and D a system of differentiable coordinates defined on G. We shall say that a *curve* $x(t)$, $|t| < \alpha$, is defined in G if there exists an element $x(t)$ which depends continuously on a real parameter t and which is such that $x(0) = e$. We shall say that the curve $x(t)$ has a *tangent* in the system of coordinates D if the derivatives

$$\frac{dx^i(0)}{dt} = a^i \tag{10}$$

exist. We shall call the numbers a^i the components of the *vector* a which is tangent to the curve $x(t)$. Of course we understand here a tangent vector at the point $t = 0$, but as other tangent vectors will not be considered, we shall omit the words "at the point $t = 0$."

When we pass from the system D to the system D' by means of relations(9), the vector a will have a new set of components in the new coordinate system which can be expressed by means of the old components as follows:

$$a'^i = p_j^i a^j \tag{11}$$

(see (8)).

By means of the above construction we associate with a local Lie group a vector space R composed of all vectors tangent to the curves in G. The connection between G and R is given by means of a definite system of coordinates D. To every transformation of coordinates (9) in G corresponds a definite transformation of coordinates (11) in R, and the connection between G and R is invariant with respect to a differentiable transformation of coordinates in G. It can readily be verified that if the curves $x(t)$ and $y(t)$ have the tangent vectors a and b, then the curve $z(t) = x(t)y(t)$ has the tangent vector $c = a + b$ (see (5)). In this way the addition of vectors in R assumes an invariant meaning.

We note here also that the dimension of the vector space R is equal to the dimension of the group G.

C) If G and G' are two differentiable or analytic local Lie groups, then their direct product H is a differentiable or analytic local Lie group.

Let D and D' be differentiable or analytic coordinates of the groups G and G'. If $x^1, \cdots, x^r$ are the coordinates of the point $x \varepsilon G$, and $x'^1, \cdots, x'^s$ are the coordinates of the point $x' \varepsilon G'$, then we take for the coordinates of the pair $(x, x') \varepsilon H$ the numbers $x^1, \cdots, x^r, x'^1, \cdots, x'^s$. If the operation of multiplication in the groups G and G' is written in coordinate form by the relations

$$z^i = f^i(x^1, \cdots, x^r; y^1, \cdots, y^r) \tag{12}$$

and

$$z'^i = f'^i(x'^1, \cdots, x'^s; y'^1, \cdots, y'^s) \tag{13}$$

then the law of multiplication in the group H can be written by means of the relations (12) and (13) taken together. This proves C).

EXAMPLE 55. Let G be the set of all square matrices of order n whose determinants are different from zero. By remark A) of §27, G is a topological group. We shall show that G is an analytic Lie group. To do this we introduce coordinates into G in the following way. We represent an arbitrary matrix $x \varepsilon G$ in the form

$$e + \|x_j^i\| \tag{14}$$

where e is the unit matrix, and the elements of the matrix $\|x_j^i\|$ are taken for the coordinates of the matrix x. The mapping thus obtained of the whole group G on an open set of the Euclidean space S of n^2 dimensions maps the identity into the origin. Relation (3) assumes for G the following algebraic form

$$z_j^i = x_j^i + y_j^i + x_k^i y_j^k. \tag{15}$$

Hence G is an analytic Lie group.

39. One-Parameter Subgroups

In the study of Lie groups an important part is played by one-parameter subgroups (see §23, M)). These subgroups are connected invariantly with the Lie group, i.e., they do not depend on the choice of coordinates in the group, and allow the introduction of a special set of coordinates into the group.

A) As we have remarked before (see §23, M)), a one-parameter subgroup of the group G is a curve $g(t)$, $|t| \leq \alpha$ (see §38, B)), which satisfies the condition

$$g(s)g(t) = g(s + t). \tag{1}$$

Two one-parameter subgroups $g(t)$ and $h(t)$ of the group G are said to *coincide* if the equation $g(t) = h(t)$ holds for sufficiently small values of t. Obviously under this condition the two subgroups really coincide for all those values of t for which they are both defined (see (1)). If now G is a local Lie group and D a differentiable coordinate system in G, then the one-parameter subgroup $g(t)$

is said to be *differentiable* in the coordinates D if the curve $g(t)$ has a tangent vector a in these coordinates (see §38, B)). We shall call the vector a the *direction vector* of the subgroup $g(t)$.

We shall now take up the question of the existence and of the uniqueness of a one-parameter subgroup with a given direction vector a. In order to formulate in detail the corresponding theorem we shall introduce the auxiliary functions

$$(2)\qquad \overset{i}{v}_j(x) = \overset{i}{v}_j(x^1, \cdots, \overset{r}{x}) = \frac{\partial}{\partial y^j} \overset{i}{f}(x^1, \cdots, \overset{r}{x}; 0, \cdots, 0)$$

(see §38, (3)).

THEOREM 46. *Let G be a local Lie group and D a differentiable system of coordinates on G. Then every one-parameter subgroup $g(t)$ having the direction vector a in the coordinates D satisfies in these coordinates the following system of equations*

$$(3)\qquad \frac{dg^i(t)}{dt} = \overset{i}{v}_j(g(t))a^j$$

(see (2)), *having for initial conditions*

$$(4)\qquad g^i(0) = 0.$$

Conversely, the solution of the system (3) *with the initial conditions* (4) *defines a one-parameter subgroup $g(t)$ having a for its direction vector. Because of the existence and the uniqueness of the solution of system* (3) *under the initial conditions* (4), *the group G contains one and only one one-parameter subgroup $g(t)$ with the direction vector a.*

PROOF. Let $g(t)$ be a one-parameter subgroup having the direction vector a. We shall show that the coordinates $g^i(t)$ of its element satisfy the system of equations (3) with the initial conditions (4).

Let us evaluate the limit

$$\lim_{s\to 0} \frac{g^i(t+s) - g^i(t)}{s} = g^{i\prime}(t).$$

From relations (1) and (3) of §38 we have

$$\overset{i}{g}(t+s) = \overset{i}{f}(g(t), g(s)) = \overset{i}{g}(t) + \overset{i}{v}_j(g(t))\overset{j}{g}(s) + \overset{i}{\epsilon}s.$$

From this equation we obtain (see §38, (4))

$$\frac{g^i(t+s) - g^i(t)}{s} = \overset{i}{v}_j(g(t))\,\frac{g^j(s)}{s} + \overset{i}{\epsilon}$$

where $\epsilon^i \to 0$ as $s \to 0$ It follows from this that the derivative $g^{i\prime}(t)$ exists and that the functions $g^i(t)$ satisfy the system (3). Since $g(0) = e$ it follows that $g^i(0) = 0$ and this gives the initial conditions (4).

Since the functions $g^i(t)$ satisfy the system (3), it follows that the group $g(t)$ with the direction vector a is unique inasmuch as the system (3) has a unique solution under the initial conditions (3). It also follows from (3) that the functions $g^i(t)$ have three continuous derivatives if the system of coordinates D is differentiable, and are analytic if the system of coordinates D is analytic.

We shall now prove the existence of the one-parameter family $g(t)$ having the direction vector a. We shall suppose that the functions $g^i(t)$ satisfy the system (3) with the initial conditions (4), and show that in this case the point $g(t)$ having the coordinates $g^i(t)$ describes a one-parameter subgroup having a direction vector a.

We note first of all that it follows from relations (5) of §38, that $dg^i(0)/dt = a^i$, i.e., the curve $g(t)$ has the tangent vector a. Hence it remains to show only that $g(t)$ is a one-parameter subgroup.

Let

$$g^*(t, u) = g(t)g(u), \tag{5}$$

and denote by $g^{*i}(t, u)$ the coordinates of the point $g^*(t, u)$. Let us estimate the difference

$$g^{*i}(t, u) - g^i(t + u) = \epsilon_1^i u \tag{6}$$

by showing that ϵ_1^i tends to zero with u.

We have

$$g^{*i}(t, u) = f^i(g(t), g(u)).$$

From this and equation (2) we get

$$g^{*i}(t, u) = g^i(t) + v_j^i(g(t))a^j u + \epsilon_2^i u, \tag{7}$$

where $\epsilon_2^i \to 0$ with u. On the other hand from (3) we have

$$g^i(t + u) = g^i(t) + v_j^i(g(t))a^j u + \epsilon_3^i u, \tag{8}$$

where $\epsilon_3^i \to 0$ with u. Our assertion about ϵ_1^i follows now from (7) and (8).

We shall now show that the functions $g^{*i}(s, t)$ satisfy the system of equations

$$\frac{\partial g^{*i}(s, t)}{\partial t} = v_j^i(g^*(s, t))a^j \tag{9}$$

with the initial conditions

$$g^{*i}(s, 0) = g^i(s). \tag{10}$$

The initial conditions (10) follow directly from (5). We shall calculate $\partial g^{*i}(s, t)/\partial t$. We have

$$g^{*i}(s, t + u) = f^i(g(s), g(t + u)).$$

From this, taking into account relation (6), we get

$$g^{*i}(s, t + u) = f^i(g(s), g^*(t, u)) + \epsilon_4^i u,$$

where $\epsilon_4^i \to 0$ as $u \to 0$. From this, and because multiplication is associative, we get

$$g^{*i}(s, t + u) = f^i(g^*(s, t), g(u)) + \epsilon_4^i u.$$

This can be written in view of (2) as follows:

$$(11) \qquad g^{*i}(s, t + u) = g^{*i}(s, t) + v_j^i(g^*(s, t))a^j u + \epsilon_5^i u,$$

where $\epsilon_5^i \to 0$ for $u \to 0$. Equation (9) follows directly from this.

On the other hand the functions $g^i(s + t)$ obviously satisfy the system of equations

$$(12) \qquad \frac{\partial g^i(s + t)}{\partial t} = v_j^i(g(s + t))a^j$$

with the initial conditions

$$(13) \qquad g^i(s + 0) = g^i(s),$$

since equations (12) coincide with equations (3).

Hence the functions $g^{*i}(s, t)$ and $g^i(s + t)$, considered, as functions of t, satisfy the same system of equations (9), (12) with the same initial conditions (10), (12). It follows from the uniqueness of the solution of this system that $g^{*i}(s, t) = g^i(s + t)$, and this means that $g(s)g(t) = g(s + t)$ (see 5)), i.e., $g(t)$ is a one-parameter subgroup. This completes the proof of Theorem 46.

B) Let G be a local Lie group. The differentiable system of coordinates D established in the neighborhood U of the identity of the group G is called a *canonical system of the first kind* if every system of equations $g^i(t) = a^i t$, $|t| \leqq \alpha$, in the coordinates D gives a one-parameter subgroup $g(t)$, $|t| \leqq \alpha$. Here the a^i are arbitrary constants and α is a positive number satisfying the sole condition that if $|t| \leqq \alpha$ then U contains a point with coordinates $a^i t$.

It can easily be seen that a linear transformation of the canonical coordinates of the first kind (see §38, A)) leads again to canonical coordinates of the first kind.

C) Let G be a local Lie group, D canonical coordinates of the first kind in G, and U an open set in which these coordinates D exist. Every one-parameter subgroup $g(t)$, $|t| \leqq \alpha$, which is differentiable in the coordinates D, and defined in G, and which satisfies the condition $g(t) \in U$ for $|t| \leqq \alpha$ can be expressed in the coordinates D by the equations

$$(14) \qquad g^i(t) = a^i t, \qquad |t| \leqq \alpha,$$

where the a^i are the coordinates of the direction vector a of the subgroup $g(t)$.

We now denote by $g^*(t)$ the point with coordinates $a^i t$, and by M the set of all positive numbers $\beta \leqq \alpha$ such that for $|t| \leqq \beta$ the point $g^*(t)$ exists. If $\beta \in M$, then by B) the curve $g^*(t)$, $|t| \leqq \beta$, is a one-parameter subgroup. Since

the direction vector of the subgroup $g^*(t)$ is obviously equal to a, it follows from Theorem 46 that $g(t) = g^*(t)$ for sufficiently small values of the parameter t. But in that case the one-parameter subgroups coincide in the whole domain of their existence (see A)), i.e., $g(t) = g^*(t)$ for $|t| \leqq \beta$. We denote by γ the least upper bound of all the numbers in the set M. Since for $|t| < \gamma$ we have $g^*(t) = g(t)$, and for $|t| = \gamma$ we have $g(t) \varepsilon U$, it follows that for $|t| = \gamma$ the point whose coordinates are a^it exists and coincides with the point $g(t)$. If now $\gamma < \alpha$ then there exists a positive ϵ such that $\gamma + \epsilon < \alpha$ and the point $g^*(t)$ is defined for all t not exceeding $\gamma + \epsilon$ in absolute value, i.e., $\gamma + \epsilon \varepsilon M$. Hence if $\gamma < \alpha$ then γ cannot be the least upper bound of all the numbers of the set M, and consequently $\gamma = \alpha$. Therefore $g(t) = g^*(t)$ for $|t| \leqq \alpha$, i.e., relations (14) are true.

THEOREM 47. *Let D be a differentiable or analytic system of coordinates of a local Lie group. Then there exists a canonical system of coordinates D' of the first kind having a transformation into the system D which is differentiable or analytic, and such that the matrix $\|p^i_j\|$ which corresponds to the transformation from coordinates D' to coordinates D* (see §38, A)) *is a unit matrix.*

PROOF. Let $g(t)$ be a one-parameter group, differentiable in coordinates D, and having the direction vector a (see Theorem 46). We put in evidence the dependence of the one-parameter subgroup $g(t)$ on the vector a by writing

$$g(t) = g(a, t). \tag{15}$$

We denote the coordinates of the point $g(t)$ in the system D by $g^i(t)$, and the coordinates of the vector a by a^i. We may then write

$$g^i(t) = g^i(a, t) = g^i(a^1, \cdots, a^r; t). \tag{16}$$

We consider the function $g(\alpha t)$ where α is a real number. The point $g(\alpha t)$ considered as a function of t describes a one-parameter subgroup since

$$g(\alpha s)g(\alpha t) = g(\alpha s + \alpha t) = g(\alpha(s + t)).$$

The direction vector of the one-parameter subgroup $g(\alpha t)$ can easily be seen to be αa. In fact

$$\frac{dg^i(\alpha t)}{dt} = \frac{dg^i(\alpha t)}{d(\alpha t)}\alpha = \alpha a^i \quad \text{for} \quad t = 0.$$

Since by Theorem 46, G contains only one one-parameter subgroup having the direction vector αa we have

$$g(a, \alpha t) = g(\alpha a, t). \tag{17}$$

This can also be written:

$$g^i(a, \alpha t) = g^i(\alpha a, t), \tag{18}$$

or

$$g^i(a^1, \cdots, a^r; \alpha t) = g^i(\alpha a^1, \cdots, \alpha a^r; t). \tag{19}$$

We note that the functions (16) are differentiable or analytic functions of all their arguments. This follows directly from the fact that they are solutions of the system of equations (3).

We now introduce the functions

$$h^i(a) = h^i(a^1, \cdots, a^r) = g^i(a^1, \cdots, a^r; 1). \tag{20}$$

We show that they are defined for all sufficiently small values of the arguments. In fact, by a well known theorem in the theory of differential equations, there exist sufficiently small numbers ϵ and δ such that for $|a^k| < \epsilon$ the solution of the system (3) is defined for $|t| < \delta$. In greater detail, the functions $g^i(a^1, \cdots, a^r; t)$, being solutions of the system (3), are defined and are differentiable or analytic for $|t| < \delta$. But in view of (19) this means that the functions (20) are defined for $|a^k| < \epsilon\delta$.

The functions (20) satisfy the condition

$$h^i(0, \cdots, 0) = 0. \tag{21}$$

In fact

$$h^i(0a^1, \cdots, 0a^r) = g^i(a^1, \cdots, a^r; 0 \cdot 1) = 0.$$

We now calculate the derivatives of the functions (20) for arguments which become zero. It is obvious that in calculating $(\partial/\partial a^j)h^i(0, \cdots, 0)$ all the arguments except a^j can be put equal to zero beforehand. We therefore assign to the vector a a special value a' by assuming that all the coordinates of the vector a are zero with the exception of the j-th coordinate, which is equal to 1. We now calculate the derivative $(d/dt)h^i(a't)$. From formulas (20) and (19) we have $h^i(a't) = g^i(a', t)$. Hence $(d/dt)h^i(a't) = (d/dt)g^i(a', t)$. Supposing that $t = 0$ in the last equation we get as the derivative $(d/dt)g^i(a', 0)$ the i-th coordinate of the direction vector a' of the subgroup $g(a', t)$. From (3) and this special choice of the vector a' we obtain in this way

$$\frac{\partial}{\partial a^j} h^i(0, \cdots, 0) = \delta^i_j. \tag{22}$$

In order to introduce the coordinates D' in the group G we consider the system of equations

$$x^i = h^i(x'^1, \cdots, x'^r) \tag{23}$$

in the unknowns x'^k. If $x^i = 0$, the system (23) has the solution $x'^k = 0$ (see equation (21)). Furthermore, the Jacobian of the system (23) is equal to unity when all the arguments equal zero (see equation (22)). Therefore the system (23) has a unique solution, which is continuous in the neighborhood of the zero values of the arguments, and therefore it can serve to introduce a new system of coordinates x'^k for the point x which had the coordinates x^i in the system D

(see §38, A)). The new system of coordinates thus obtained we shall denote by D'.

We consider in the group G a curve $g^*(t)$ given linearly in the coordinates D' as follows:

$$g^{*i}(t) = a^i t. \tag{24}$$

Let us consider the form of this curve in the coordinates D. To do this we substitute in equation (23) the expression $a^k t$ for x'^k and get

$$x^i = h^i(a^1 t, \cdots, a^r t) = g^i(a^1, \cdots, a^r; t)$$

(see (20) and (19)). This shows that the curve $g^*(t)$ under consideration is a one-parameter subgroup. Hence any curve given in D' coordinates by equations (24) is a one-parameter subgroup, and therefore the coordinates D' constitute a canonical system of the first kind (see B)).

Since the functions (16) are differentiable or analytic the functions (20) possess the same property, and therefore the transformation from D' coordinates to D coordinates is correspondingly differentiable or analytic.

Hence Theorem 47 is proved.

The following Theorem 48 shows that every one-parameter subgroup is differentiable in any differentiable system of coordinates. In this way Theorem 48 is the first step towards the proof of the differentiability of certain functions for which differentiability was not presupposed.

THEOREM 48. *If D is a system of differentiable coordinates in the local group G, then every one-parameter subgroup $g(t)$ of the group G is differentiable in the coordinates D.*

PROOF. Since by Theorem 47 it is possible by means of a differentiable transformation to go from the coordinates D to a set of canonical coordinates of the first kind, we can suppose without loss of generality that the coordinates D themselves are canonical of the first kind.

We denote by V that neighborhood of the identity e of the group G in which the coordinates D are defined. We now denote by U_α the set of elements of V whose coordinates satisfy the relations

$$|x^i| < \alpha. \tag{25}$$

Obviously there exists a positive number ϵ such that for $\alpha = \epsilon$ there corresponds to every system x^i satisfying equation (25) a point of V. Let $U_\epsilon = U$. There also exists a positive number δ such that

$$U_\delta^2 \subset U, \tag{26}$$

and such that the product of any two elements of U_δ is defined (see §23, E)). We set $U_\delta = U'$.

Let t' be a sufficiently small positive number such that

$$(27) \qquad g(t) \in U' \quad \text{for} \quad |t| \leqq t'.$$

We denote the coordinates of the point $g(t)$ in the system D by $g^i(t)$. Furthermore, let n be a positive integer. We set

$$(28) \qquad a_n^i = \frac{n}{t'} g^i\left(\frac{t'}{n}\right)$$

and denote the vector whose coordinates are a_n^i by a_n, and the one-parameter subgroup having the direction vector a_n (see Theorem 46) by $g_n(t)$, while the coordinates of the point $g_n(t)$ we denote by $g_n^i(t)$. Since the coordinates D are canonical it follows that

$$(29) \qquad g_n^i(t) = a_n^i t.$$

It should be remembered that equations (29) hold only for sufficiently small values of the parameter t, in fact only as long as the curve $g_n(t)$ remains in the region V (see C)) in which the coordinates D were defined. The curve $g_n(t)$ may leave the region V and return to it again and the point $g_n(t)$ will again have coordinates, but they will not be defined by equations (29).

We now take up the question: for what values of the parameter t do equations (29) hold? We shall show that they hold for all values of t for which $|t| \leqq t'$.

Since for $|t| \leqq t'$, $g(t) \in U'$, it follows that $g(t'/n) \in U'$, and therefore $|g^i(t'/n)| < \delta$. It follows from this that $|a_n^i t| < \delta$ for $|t| \leqq t'/n$ (see (28)). Hence for $|t| \leqq t'/n$ we have

$$(30) \qquad g_n(t) \in U'$$

and equations (29) have a meaning for these values of the parameter. We get from equations (28) and (29) that $g_n^i(t'/n) = g^i(t'/n)$ and hence

$$(31) \qquad g_n(t'/n) = g(t'/n).$$

Now let m be a positive integer which does not exceed n. Raising equation (31) to the m-th power we get

$$(32) \qquad g_n\left(\frac{m}{n} t'\right) = g\left(\frac{m}{n} t'\right),$$

where the left side exists because of the existence of the right side. We now consider a positive number t which does not exceed t'. This number can be written in the form $t = (m/n)t' + s$, where $m \leqq n$ and $0 \leqq s < t'/n$. It follows from equation (1) that

$$g_n(t) = g_n\left(\frac{m}{n} t'\right) g_n(s) = g\left(\frac{m}{n} t'\right) g_n(s).$$

By (27), $g((m/n)t') \in U'$, and by (30) we have $g_n(s) \in U'$, and therefore

$g_n(t) \in U'U' \subset U$. Hence for $|t| \leq t'$ we have $g_n(t) \in U$, and equations (29) have a meaning for all t such that $|t| \leq t'$.

Supposing that $m = n$ in (32) we get $g_n(t') = g(t')$. Writing this equation in coordinate form, which is possible by what we have just proved, we get $a_n^i t' = g^i(t')$. Hence a_n^i does not depend on the number n and therefore the group $g_n(t)$ does not depend on n, and we can denote it by $g^*(t)$. Equation (32) can then be written

$$g^*\left(\frac{m}{n}\, t'\right) = g\left(\frac{m}{n}\, t'\right) \tag{33}$$

where m and n, $m \leq n$, are arbitrary positive integers. Since the elements of the groups $g^*(t)$ and $g(t)$ are continuous functions of t, it follows from (33) that $g^*(t) = g(t)$, and this means that the group $g(t)$ coincides with the differentiable group $g^*(t)$. Hence Theorem 48 is proved.

Theorem 48 can be thought of as the first invariance theorem. It shows that every one-parameter subgroup has a direction vector in any differentiable coordinates.

40. Invariance Theorem

We shall show here that if a Lie group has two differentiable systems of coordinates, then these system are connected by a differentiable transformation. The significance of this proposition has already been explained in §38. It forms the basis for a coordinate study of Lie groups. In fact, when we investigate the law of multiplication of a group from the point of view of coordinates, we actually study the properties of the system of equations (3) of §38. In order to study the properties of the group itself, we must look for those properties of this system which remain invariant under a transformation of coordinates. Theorem 49 below shows that we need only consider differentiable transformations of coordinates.

To prove Theorem 49 we introduce canonical coordinates of the second kind (see A)).

We note here that the dimension r of the Lie group G was defined by means of coordinates (see Definition 38), and therefore if we do not wish to refer to the topological theorem of the invariance of the number of dimensions, we cannot as yet assert that the dimension is an invariant of the group G. Therefore we shall speak here of the dimension of the group G with respect to a given system of coordinates. We also recall that the dimension of the group G in the coordinates D is equal to the dimension of the vector space R associated with the group G by means of the coordinates D (see §38, B)).

We now pass to the construction of canonical coordinates of the second kind.

A) Let G be a local Lie group and D a system of differentiable or analytic coordinates defined in G; and let the dimension of the group G be equal to r in these coordinates. We shall say that a set of one-parameter subgroups of the group G are *linearly independent in the coordinates D* if their direction vec-

tors are linearly independent in the system D. We select in G a system of r one parameter subgroups,

(1) $$g_1(t), \cdots, g_r(t), \qquad |t| \leqq \alpha,$$

which are linearly independent in the coordinates D. We consider the points

(2) $$g(t^1, \cdots, t^r) = g_1(t^1) \cdots g_r(t^r), \qquad |t^k| < \beta \leqq \alpha,$$

which exist for sufficiently small values of β.

If β is chosen sufficiently small, then the points of the type (2) form a neighborhood U of the identity in the group G such that every point of U can be uniquely represented in the form (2), i.e., it defines the numbers t^k. Therefore if we take the numbers t^k for the coordinates of the point $g(t^1, \cdots, t^r) \varepsilon U$, we shall introduce into G a new system of coordinates D', which is called a *canonical system of the second kind.*

We can then show that there exists a differentiable or an analytic transformation of D into D' according as the original system D was differentiable or analytic, respectively.

In order to prove A) we denote by $g_k^i(t)$ the coordinates of the point $g_k(t)$ in the system D, by $g^i(t^1, \cdots, t^r)$ the coordinates of the point $g(t^1, \cdots, t^r)$ in the system D, and by a_k^i the coordinates of the direction vector a_k of the group $g_k(t)$ in the system D.

The transition from the system D' to the system D is effected by

(3) $$x^i = g^i(t^1, \cdots, t^r),$$

where the x^i are the coordinates of the point x in the system D while the t^k are the coordinates of the same point in the system D'. To prove A) we show that the system (3) satisfies the conditions of Definition A) of §38.

The system (3) is differentiable or analytic. This follows from Theorem 46.

Since $g_k(0) = e$, it follows that $g(0, \cdots, 0) = e$, and hence $g^i(0, \cdots, 0) = 0$.

We now calculate the derivative $(\partial/\partial t^k)g^i(t^1, \cdots, t^r)$ when the arguments all become zero. In this calculation we can suppose that all the arguments except one, t^k, are already zero, and then find the derivative with respect to t^k. We therefore obtain

$$\frac{\partial}{\partial t^k} g^i(t^1, \cdots, t^r) = \frac{\partial}{\partial t} g_k^i(t) = a_k^i \quad \text{for} \quad t^i = t = 0.$$

Hence the Jacobian of the system (3) is equal to the determinant of the matrix $\|a_k^i\|$, which is different from zero because of the linear independence of the selected system of subgroups (1).

Hence the system of equations (3) has a solution in a small neighborhood of zero, and therefore assertion A) is proved.

Before taking up Theorem 49 we make one more preliminary remark.

B) Let G be a local Lie group, D and D' two differentiable systems of coordinates defined in G, and R and R' the vector spaces associated with G by means

of the coordinate systems D and D' (see §38 B)). Let $g(t)$ be a one-parameter subgroup of G, and a and a' its direction vectors in the coordinates D and D' (see Theorem 48), $a \varepsilon R$, $a' \varepsilon R'$. The one-to-one correspondence $a \rightleftarrows a'$ thus obtained between the spaces R and R' is bicontinuous. Therefore a topology can be introduced in a natural way into the set of all one-parameter subgroups of the group G independently of any coordinate system. The proximity of two subgroups is defined as the proximity of their direction vectors in any differentiable system of coordinates.

It follows from Theorem 47 that we can assume without loss of generality that D and D' are canonical systems of the first kind. To prove the continuity of the mapping $a \to a'$ in the neighborhood of some definite vector a, we select a sufficiently small number τ such that a point with coordinates $a^i\tau$ in the system D and a point with coordinates $a'^i\tau$ in the system D' are defined and both coincide with the point $g(\tau)$ (see §39, B) and C)). To a small change in the vector a there obviously corresponds a small change in the point $g(\tau)$, and to a small change in $g(\tau)$ correspond small changes in the coordinates $a'^i\tau$, i.e., a small change in the vector a'. Hence the mapping $a \to a'$ is continuous. The continuity of the mapping $a' \to a$ is proved in the same way.

THEOREM 49. *Let D and D' be two systems of coordinates in a local Lie group G. We suppose that they are both either differentiable or analytic, We denote by r and s the dimensions of G in the coordinates D and D', respectively. Then $r = s$, and there exists a differentiable or analytic transformation of coordinates D to coordinates D'* (see §38, A)), *i.e., the transformation of the coordinate system D to D' is given by*

$$x'^i = \varphi^i(x^1, \cdots, x^r), \tag{4}$$

where the functions on the right hand side are differentiable or analytic, and the Jacobian of the system (4) *does not become zero when the arguments assume zero values.*

PROOF. Suppose that $r \leqq s$. We select, as in A), a system of r linearly independent one-parameter subgroups in the coordinates D,

$$g_1(t), \cdots, g_r(t). \tag{5}$$

These subgroups will have direction vectors in the coordinates D' (see Theorem 48), but it is not at all obvious that the one-parameter subgroups (5) will be linearly independent in the coordinates D'. Since $s \geqq r$, it is possible by a slight change in these subgroups to make them linearly independent in D'. This change, being arbitrarily small, will not affect the linear independence of the subgroups (5) in the coordinates D. Hence the subgroups (5) are linearly independent in both sets of coordinates D and D'. In case $s > r$ we adjoin to the system (5) the one-parameter groups $g_{r+1}(t), \cdots, g_s(t)$ in such a way that the new system

$$g_1(t), \cdots, g_r(t), g_{r+1}(t), \cdots, g_s(t) \tag{5'}$$

is linearly independent in the coordinates D'.

The systems (5) and (5′) of one-parameter subgroups can be taken as bases for the construction for canonical coordinate systems D^* and D'^* of the second kind. Let

$$t'^1, \cdots, t'^r, t'^{r+1}, \cdots, t'^s \tag{6}$$

be a system of arbitrarily small numbers. If these numbers are sufficiently small then there exists a point x whose coordinates in the system D'^* are numbers of the system (6). Also, if the numbers of the system (6) are sufficiently small, then the coordnates of the points x are defined in the system D^*; we denote them by

$$t^1, \cdots, t^r.$$

We now have

$$g_1(t^1) \cdots g_r(t^r)g_{r+1}(0) \cdots g_s(0) = g_1(t'^1) \cdots g_r(t'^r)g_{r+1}(t'^{r+1}) \cdots g_s(t'^s).$$

If we consider this equation from the point of view of the coordinate system D'^*, we conclude that the point x has in this system the coordinates $t^1, \cdots, t^r, 0, \cdots, 0$, and at the same time the coordinates $t'^1, \cdots, t'^r, t'^{r+1}, \cdots, t'^s$. This is possible only when $t'^{r+1} = \cdots = t'^s = 0$. This last equation contradicts the assumption that the numbers of the system (6) are arbitrary, although sufficiently small. Hence the assumption that $s > r$ has led to a contradiction. Therefore $s = r$, and the systems (5) and (5′) of one-parameter subgroups coincide, which means that the coordinate systems D^* and D'^* also coincide.

By A) there exists a differentiable or analytic transformation from the system D to the system D^*. In the same way there exist a differentiable or analytic transformation from the system D' to the system D'^*. Since, as we have just shown, $D^* = D'^*$, it follows that there exists a differentiable or analytic transformation from the system D to the system D'.

This proves Theorem 49.

Example 56. Let G be a commutative Lie group. We introduce into G canonical coordinates of the second kind. We denote the elements having the coordinates t^i by $g(t^1, \cdots, t^r)$. It is not hard to see that the product of two elements can be expressed by the formula

$$g(s^1, \cdots, s^r)g(t^1, \cdots, t^r) = g(s^1 + t^1, \cdots, s^r + t^r).$$

This shows that the commutative group G is locally isomorphic with a vector group (see Definition 30).

41. Subgroup and Factor Group

We shall show in this section that every subgroup H of the Lie group G is also a Lie group, and that H is a differentiable manifold in the manifold G. We shall also show that every factor group G^* of the Lie group G is also a Lie

group, and that a natural homomorphic mapping of the group G on the group G^* can be given by means of differentiable functions. It will be proved here that in considering subgroups and factor groups we can limit ourselves to differentiable functions.

THEOREM 50. *A subgroup H* (see §23, I)) *of a local Lie group G is also a local Lie group, and H is a differentiable or analytic Lie group according as the group G is differentiable or analytic. We denote by D and E arbitrary systems of coordinates in the groups G and H. We shall suppose that D and E are either both differentiable or both analytic. Let $y^1, \cdots, y^s$ be the coordinates of the point $y \in H$ in the system E, and $x^1, \cdots, x^r$ the coordinates of the same point in the system D. Then we have*

$$(1) \qquad x^i = \psi^i(y^1, \cdots, y^s), \qquad i = 1, \cdots, r,$$

where the functions in the right side of equation (1) *are differentiable or analytic. Furthermore let*

$$(2) \qquad q^i_j = \frac{\partial}{\partial y^j} \psi^i(0, \cdots, 0).$$

Then the rank of the matrix $\|q^i_j\|$ is equal to s, i.e., in particular $s \leqq r$.

In short, Theorem 50 can be formulated by saying that a subgroup of a local Lie group is also a local Lie group, and is a differentiable or analytic manifold of the correspondingly differentiable or analytic manifold G.

PROOF. Let D' be a system of canonical coordinates of the first kind in G (see §39, B)), and V the open set in which they exist. We denote the dimension of the group G by r, and the coordinates of the point $x \in V$ by x^i in the system D'. We denote by U_α the set of all the points x for which the following inequality holds:

$$x^1x^1 + \cdots + x^rx^r < \alpha^2,$$

where α is a positive number. There exists a sufficiently small number β such that any set of numbers y^i which satisfy the inequality $y^1y^1 + \cdots + y^ry^r \leqq \beta^2$ defines a point $y \in V$ with coordinates y^i. There also exists a sufficiently small number $\gamma \leqq \beta$ such that the product of any $r + 1$ elements of $\bar{U}_\gamma$ is defined, and if these elements belong to H then their product also belongs to H, (see §23, E)). Finally there exists a sufficiently small number $\delta \leqq \gamma$ such that the set $\bar{U}_\delta \cap H$ is closed in $\bar{U}_\delta$. We shall make use of all these conditions of smallness in what follows. In order not to introduce unnecessary complications into the calculations we shall suppose that δ is equal to unity. This is permissible since we can always change the scale of the construction by an appropriate transformation of coordinates.

Let $b \in U_1$ be an element of H whose coordinates in the system D' we denote by b^i. Let $\rho = \sqrt{(b^1b^1 + \cdots + b^rb^r)}$. We shall show that if m is an integer

satisfying the inequality $m\rho < 1$, then the element $(b)^m$ has the coordinates mb^i and belongs to H,

$$(b)^m \varepsilon H \quad \text{for} \quad m\rho < 1. \tag{3}$$

We consider the one-parameter subgroup $g(t)$, $|t| < 1/\rho$, the coordinates of whose direction vector are the numbers b^i. We then have $g^i(t) = b^it$, $|t| \leqq 1/\rho$ (see §39, B)). Hence $b = g(1)$. Let p be an integer not exceeding m. Raising the relation $b = g(1)$ to the p-th power, we get $(b)^p = g(p)$, i.e., the coordinates of the elements $(b)^p$ are the numbers pb^i. This element exists since $p < 1/\rho$. We shall show that all the elements b, $(b)^2, \cdots, (b)^m$ belong to H. The proof is by induction. Let $p + 1 \leqq m$ so that $(b)^p \varepsilon U_1$, and suppose that $(b)^p \varepsilon H$. Then the product $b(b)^p$ is defined and belongs to H since both factors belong to U_1 and to H. Therefore $(b)^{p+1} \varepsilon H$.

Theorem 50 is obviously true in case the identity e of the group G is an isolated element of the group H. For then $s = 0$ and relation (1) becomes $x^i = 0$.

We now make the following inductive assumption. Suppose that for some non-negative k there exists a system of one-parameter subgroups

$$g_1(t), \quad \cdots, g_k(t) \tag{4}$$

which has the following properties: 1) the element $g_j(t)$ belongs to H for $|t| \leqq 1, j = 1, \cdots, k$; 2) The direction vectors $a_1, \cdots, a_k$ of the subgroups of the system (4) are orthogonal unit vectors in the system of coordinates D'; if we denote the coordinates of the vector a_j by a_j^i, then

$$\sum_{i=1}^{r} a_p^i a_q^i = \delta_{pq}. \tag{5}$$

Obviously $k \leqq r$.

Our inductive assumption is obviously true for $k = 0$. Suppose that it is true for a given k. We denote by H_k the set of all elements of the form

$$g(t^1, \cdots, t^k) = g_1(t^1) \cdots g_k(t^k), \qquad |t^j| \leqq 1, \qquad j = 1, \cdots, k. \tag{6}$$

If $k = 0$ we let $H_k = \{e\}$.

The set H_k is entirely contained in H inasmuch as every element $g_j(t^j)$ belongs to H and to U_1 and $k \leqq r$ by hypothesis. We shall now show that there exist two mutually exclusive cases: a) the set H_k contains some neighborhood of the identity of the group H, b) the system of subgroups (4) can be enlarged by adjoining one more subgroup in such a way that the inductive assumptions will hold for the enlarged system.

We denote by L_k the set of all elements of U_1 for which the coordinates $x^1, \cdots, x^r$ satisfy the linear relations

$$\sum_{i=1}^{r} a_j^i x^i = 0, \qquad j = 1, \cdots, k. \tag{7}$$

If $k = 0$ we suppose that $L_k = U_1$. We denote by

$$g(t^1, \cdots, t^k; x) \tag{8}$$

the element $g(t^1, \cdots, t^k)x^{-1}$, where $x \in U_1$. The set of all elements of the form (8) for a fixed x and for $|t_j| \leq 1$, $j = 1, \cdots, k$, is the set $H_k x^{-1}$.

We consider the intersection of the sets L_k and $H_k x^{-1}$ with respect to the element x, for x in the neighborhood of e.

To do this we denote by $g^i(t^1, \cdots, t^k; x)$ the coordinates of the element (8). In order to find the intersection of the sets L_k and $H_k x^{-1}$ it is sufficient to solve with respect to the parameters $t^1, \cdots, t^k$ the system of equations

$$\sum_{i=1}^{r} \overset{i}{a}_j \overset{i}{g}(\overset{1}{t}, \cdots, \overset{k}{t}; x) = 0, \qquad j = 1, \cdots, k. \tag{9}$$

For $x = e$ this system has the obvious solution $t^j = 0$, $j = 1, \cdots, k$. In order to clarify the question of the solution of the system (9) we calculate the Jacobian of this system for $t^p = 0$, $p = 1, \cdots, k$, $x = e$. Under these conditions we have

$$\frac{\partial}{\partial t^j} g^i(\overset{1}{t}, \cdots, \overset{k}{t}; x) = \frac{d}{dt} \overset{i}{g}_j(t) = \overset{i}{a}_j \quad \text{for} \quad t = 0. \tag{10}$$

Hence for $t^p = 0$, $p = 1, \cdots, k$, $x = e$ we have

$$\frac{\partial}{\partial t^j} \sum_{i=1}^{r} \overset{i}{a}_h \overset{i}{g}(\overset{1}{t}, \cdots, \overset{k}{t}; x) = \sum_{i=1}^{r} \overset{i}{a}_h \overset{i}{a}_j = \delta_{hj}$$

(see (10) and (5)). Hence for x in the neighborhood of e there exists only one solution of the system (9) which is in the neighborhood of the original solution, and which depends continuously on x. This means that if x is sufficiently close to e then there exists one and only one point of intersection of the sets L_k and $H_k x^{-1}$ which is close to e, and that this point $\varphi(x)$ depends continuously on x and $\varphi(e) = e$.

Let us suppose that assumption a) is not fulfilled. Then there exists a sequence

$$b_1, b_2, \cdots, b_n, \cdots \tag{11}$$

of elements of the group H which converges to the identity e and is such that its elements do not belong to the set H_k. Let $c_n = \varphi(b_n)$. Since the function $\varphi(x)$ is continuous and since $\varphi(e) = e$, the sequence

$$c_1, c_2, \cdots, c_n, \cdots \tag{12}$$

converges to e. All the points of this sequence belong to L_k since $\varphi(x) \in L_k$. Furthermore, they all belong to H. In fact $c_n \in H_k b_n^{-1} \subset H$ since $b_n^{-1} \in U_1$. We note another important fact, namely, that no element of the sequence (12)

equals e. For if we suppose that $c_n = e$ we get $e \varepsilon H_k b_n^{-1}$, but then $b_n \varepsilon H_k$, which contradicts our assumption.

We shall use system (12) together with the properties just established, namely:

$$c_n \varepsilon L_k, \qquad c_n \varepsilon H, \qquad c_n \neq e, \quad \lim_{n\to\infty} c_n = e, \tag{13}$$

as the foundation of the following construction. We denote the coordinates of the point c_n of the sequence (12) by

$$\overset{i}{c}_n \tag{14}$$

and suppose further that

$$\rho_n = \sqrt{(\overset{1}{c}_n\overset{1}{c}_n + \cdots + \overset{r}{c}_n\overset{r}{c}_n)}. \tag{15}$$

The point with coordinates

$$\frac{1}{\rho_n}\overset{i}{c}_n = \overset{\prime i}{a}_n \tag{16}$$

we denote by a_n'. It is not hard to show that the point a_n' lies on the intersection of the set $\overline{L}_k$ and the boundary of the neighborhood U_1. Therefore there exists a point a which is a limit point of the sequence

$$a_1', a_2', \cdots, a_n', \cdots, \tag{17}$$

and a also lies on the intersection of the set $\overline{L}_k$ and the boundary of the neighborhood U_1. We denote by $\overset{i}{a}_{k+1}$ the coordinates of the point a in the system D'. These coordinates satisfy the system of equations (7) since $a \varepsilon \overline{L}_k$. Moreover

$$\overset{1}{a}_{k+1}\overset{1}{a}_{k+1} + \cdots + \overset{r}{a}_{k+1}\overset{r}{a}_{k+1} = 1,$$

since a belongs to the boundary of the neighborhood U_1.

We consider the one-parameter subgroup $g_{k+1}(t)$ defined by the relations $\overset{i}{g}_{k+1}(t) = \overset{i}{a}_{k+1}t$, $|t| \leqq 1$. The direction vector of this subgroup has the coordinates $\overset{i}{a}_{k+1}$, and therefore if we adjoin the subgroup $g_{k+1}(t)$ to the system (4) the inductive assumption 2) will still hold for the enlarged system. It can also readily be seen that the subgroup $g_{k+1}(t)$ satisfies the inductive assumption 1). In fact the point $c_n \varepsilon H$ has the coordinates $\rho_n \overset{\prime i}{a}_n$ (see (16)). From this it follows that $(c_n)^m \varepsilon H$ and has coordinates $m\rho_n \overset{\prime i}{a}_n$ if $m\rho_n < 1$ (see (3)). Now let t be a real number satisfying the inequalities $0 < t \leqq 1$. Since the sequence (17) has the limit point a, and since $\lim_{n\to\infty}\rho_n = 0$ (see (13)), we can find integers m and n such that $m\rho_n < 1$ and $|t\overset{i}{a}_{k+1} - m\rho_n\overset{\prime i}{a}_n| < \epsilon$, where ϵ is a preassigned positive number. Hence the point $g_{k+1}(t)$ is a limit point for points of the form $(c_n)^m \varepsilon \overline{U}_1 \cap H$, and since $\overline{U}_1 \cap H$ is closed in $\overline{U}_1$ it follows that $g_{k+1}(t) \varepsilon H$.

Thus we have shown that either the case a) or the case b) holds.

The above inductive construction enables us, beginning with $k = 0$, to enlarge the system (4) to a system

$$(18) \qquad g_1(t), \cdots, g_s(t) \quad \text{where} \quad k = s \leqq r,$$

and condition a) is satisfied for the whole system (18). The direction vectors $a_1, \cdots, a_s$ of the system (18) are linearly independent because of the orthogonality conditions (5). If $s < r$ we can enlarge the system (18) to a complete linearly independent system

$$(19) \qquad g_1(t), \cdots, g_s(t), g_{s+1}(t), \cdots, g_r(t).$$

By remark A) of §40 the system (19) can be taken as the basis of canonical coordinates D^* of the second kind in G.

Condition a) is satisfied for the system (18), and hence there exists a neighborhood W of the identity in the group H such that $W \subset H_s$. Since the set of all open sets of the form U_α forms a complete system of neighborhoods of the identity in G, there exists a sufficiently small positive number α' such that the intersection $H \cap U_{\alpha'}$ is entirely contained in W, and hence in H_s. Moreover, we can suppose that α' is so small that the coordinates D^* are defined in the neighborhood $U_{\alpha'}$. If now y is a point of H belonging to $U_{\alpha'}$, then its coordinates in the system D^* are the numbers $t^1, \cdots, t^s, 0, \cdots, 0$. We can take the numbers $t^1, \cdots, t^s$ as coordinates of the point y in the group H. In this way we obtain a coordinate system E^* in the group H. It can readily be seen that the coordinates E^* thus obtained in the group H are differentiable or analytic according as the coordinates D^* are differentiable or analytic. Relation (1) holds obviously for the systems D^* and E^*, and has the particularly simple form

$$(20) \qquad x^1 = y^1, x^2 = y^2, \cdots, x^s = y^s, x^{s+1} = 0, \cdots, x^r = 0.$$

If D is a system of differentiable coordinates in G, then by Theorem 49 there exists a differentiable transformation from it to the system D^*. If, on the other hand, the system D is analytic, then by remark A) of §40 the transformation from D to D^* will be analytic. For the same reason, the transformation from a system E of H to E^* will be correspondingly differentiable or analytic. Combining in the proper way the transformations from one system of coordinates to another we can obtain formula (1), which also satisfies the conditions of Theorem 50, from formula (20).

This completes the proof of Theorem 50.

THEOREM 51. *Let G be a local Lie group of r-dimensions, and H a factor group of the group G* (see §23, J)). *Then H is also a local Lie group, differentiable or analytic according as G is differentiable or analytic. We denote by χ the natural local homomorphic mapping of the group G on the group H* (see §23, K)), *and by D and E coordinate systems in the groups G and H which are either both differentiable*

or both analytic. Then the homomorphism χ *can be expressed by means of the coordinates* D *and* E *as follows:*

$$(21)\qquad y^j = \chi^j(x^1, \cdots, x^r), \qquad j = 1, \cdots, s,$$

where the functions on the right side of the equations are differentiable or analytic. Furthermore let

$$(22)\qquad r_i^j = \frac{\partial}{\partial x^i} \chi^j(0, \cdots, 0).$$

Then the rank of the matrix $\|r_i^j\|$ *is equal to* s*, i.e., in particular* $s \leqq r$*, and the kernel of the homomorphism* χ *has* $(r - s)$ *dimensions.*

PROOF. We denote by N the kernel of the homomorphism χ. By Theorem 50, N is a local Lie group. Suppose the dimension of the group N is $r - s$, and denote by

$$(23)\qquad g_{s+1}(t), \cdots, g_r(t)$$

a system of $r - s$ linearly independent one-parameter subgroups of the group N (see §40, A)). By Theorem 50, the subgroups (23) are also linearly independent in the group G. Hence the system (23) can be enlarged to form a system

$$(24)\qquad g_1(t), \cdots, g_s(t), g_{s+1}(t), \cdots, g_r(t),$$

in such a way that the new system is composed of linearly independent subgroups in G. We shall use the system (24) as the basis for the construction of a canonical system D^* of the second kind in G (see §40, A)).

We denote by K the set of all those elements of G for which the last $r - s$ coordinates become zero in the system D^*. It can be seen easily that every element $x \,\varepsilon\, G$ which is sufficiently close to the identity decomposes uniquely into a product

$$(25)\qquad x = uv,$$

where $u \,\varepsilon\, K$, $v \,\varepsilon\, N$. Furthermore, two elements $x = uv$ and $x' = u'v'$ which are sufficiently close to the identity belong to the same coset of N if and only if $u = u'$. In fact if $u = u'$, we have $x^{-1}x' = v^{-1}v' \,\varepsilon\, N$. Conversely, if x and x' belong to the same coset, then $x' = xw$, where $w \,\varepsilon\, N$, and hence $x' = uvw$, where $u \,\varepsilon\, K$, $vw \,\varepsilon\, N$, i.e., because of the uniqueness of the decomposition (25) we have $u' = u$. This remark shows that all the elements which belong to one and the same coset X of the subgroup N have their first s coordinates in common. We shall take these first s coordinates for the coordinates of the coset X. We denote the system of coordinates thus obtained in H by E^*.

Let X and X' be two cosets, and let $t^1, \cdots, t^s$ and $t'^1, \cdots, t'^s$ be their coordinates in the system E^*. We now denote by x the elements with the coordinates

$$(26)\qquad t^1, \cdots, t^s, 0, \cdots, 0$$

in the system D^*, and by x' the element with the coordinates

$$t'^1, \cdots, t'^s, 0, \cdots, 0 \tag{27}$$

in the same system. Then $x \in X$, $x' \in X'$. We denote by

$$t''^1, \cdots, t''^s \tag{28}$$

the first s coordinates of the product $xx' = x''$ in the system D^*. Then the coordinates of the coset $X'' = XX'$ in the system E^* will be equal to (28). Since the numbers (28) are obtained from the numbers (26) and (27) by means of those operations which form a product in the system D^*, it follows that the coordinates E^* are differentiable or analytic according as the coordinates D^* are differentiable or analytic. Hence H is a Lie group.

In the coordinates D^* and E^* relations (21) become

$$y^1 = x^1, \cdots, y^s = x^s. \tag{29}$$

It is clear that this relation satisfies the conditions of Theorem 51. In going from the coordinates D^* and E^* to arbitrary coordinates D and E we can make sure that Theorem 51 is also true for them by using Theorem 49 and remark A) of §40, just as was done in the proof of Theorem 50. This completes the proof of Theorem 51.

Theorems 49, 50, and 51 show that from now on in studying Lie groups we can confine our attention to differentiable functions only.

We give here one rather important corollary to Theorem 50.

A) Let G be the set of all complex square matrices of order n with non-zero determinants. From remark A) of §27, G is a topological group. It can be shown that G is also an analytic Lie group. Hence by Theorem 50 every subgroup of the group G is also an analytic Lie group.

In order to introduce coordinates into the group G, the matrix $x \in G$ can be written in the form

$$x = e + \left\| x_k^{\prime j} + i x_k^{\prime\prime j} \right\| \tag{30}$$

where e is the unit matrix, $i = \sqrt{-1}$, and $x_k^{\prime j}$ and $x_k^{\prime\prime j}$ are real numbers. We shall take these numbers as coordinates of the matrix x. Hence the dimension of G is $2n^2$. If x, y, and z are three matrices, and if $z = xy$, then in coordinate form this relation may be written

$$z_k^{\prime j} = x_k^{\prime j} + y_k^{\prime j} + x_\alpha^{\prime j} y_k^{\prime \alpha} - x_\alpha^{\prime\prime j} y_k^{\prime\prime \alpha}, \quad z_k^{\prime\prime j} = x_k^{\prime\prime j} + y_k^{\prime\prime j} + x_\alpha^{\prime j} y_k^{\prime\prime \alpha} + x_\alpha^{\prime\prime j} y_k^{\prime \alpha}. \tag{31}$$

Since these relations are analytic, the group G is an analytic Lie group.

42. Supplementary Remarks about Canonical Coordinates

If we make use of canonical coordinates of the first kind (see §39, B)), then the relations appearing in Theorems 49, 50, and 51 are linear and can be obtained rather simply. To prove this we give a preliminary proposition.

A) Let us consider a differentiable function

$$f(z^1, \cdots, z^k) \tag{1}$$

defined in the neighborhood of arguments which approach zero and such that

$$f(0, \cdots, 0) = 0. \tag{2}$$

Let us further suppose that the function (1) is homogeneous, that is, if $z^i = c^i t$, $i = 1, \cdots, k$, where $c^1, \cdots, c^k$ are arbitrary constants and t is a parameter, then the function

$$f(c^1 t, \cdots, c^k t) = ct \tag{3}$$

is a linear function of the parameter t. Under these conditions the function (1) is linear, i.e.,

$$f(z^1, \cdots, z^k) = p_1 z^1 + \cdots + p_k z^k,$$

where $p_1, \cdots, p_k$ are constants.

Let $c^1, \cdots, c^k$ be a system of arbitrary but sufficiently small numbers. Then relation (3) has a meaning for $t = 1$, and we get

$$c = f(c^1, \cdots, c^k). \tag{4}$$

Differentiating relation (3) with respect to t and letting $t = 0$, we get

$$c = \sum_{i=1}^{k} \frac{\partial}{\partial z^i} f(0, \cdots, 0) c^i. \tag{5}$$

Since in relations (4) and (5) the numbers $c^1, \cdots, c^k$ are arbitrary and sufficiently small we see that (1) is a linear function.

B) If we now assume the systems of coordinates considered in Theorems 49, 50, 51 to be canonical of the first kind, then relation (4) of §40, and (1) and (21) of §41 assume a linear form and become

$$x'^i = p^i_j x^j \tag{6}$$

$$x'^i = q^i_j y^j \tag{7}$$

$$y^j = r^j_i x^i. \tag{8}$$

The proof of proposition B) follows directly from remark A). On the right sides of relation (4) of §40, and relations (1) and (21) of §41, we put the coordinates of a point which describes a one-parameter subgroup. Since all the coordinates under consideration are canonical of the first kind, it follows that all the arguments and functions become linear functions of the parameter t and remark A) can be applied in this case.

CHAPTER VII

THE STRUCTURE OF COMPACT TOPOLOGICAL GROUPS

The object of the classical theory of continuous groups is the study of Lie groups (see Definition 38). These groups have been studied in considerable detail, and it is therefore advisable to establish the connection between general topological groups and Lie groups. It turns out that it is possible by means of a certain limiting process to construct any compact topological group satisfying the second axiom of countability from compact Lie groups (see Theorem 54). Therefore, questions about topological groups of a rather general character can be reduced to corresponding questions concerning Lie groups. In particular, it is possible to single out compact Lie groups from general topological groups by imposing certain conditions of a rather general character (see Theorems 56 and 57). All these results depend entirely on Theorem 28 of the fourth chapter. Since no analogue of Theorem 28 has as yet been found for locally compact groups, the methods which are applicable to compact groups cannot be generalized to locally compact groups, and many of the fundamental problems are still open for these groups.

The problem of distinguishing Lie groups from topological groups of a more general type was formulated by Hilbert. Modernizing a little the statement of this problem without, however, altering its meaning, we can formulate the problem as follows:

We shall call a topological group G a *parameter* group if there exists a neighborhood U of the identity of the group G which is homeomorphic with n-dimensional Euclidean space. This means that coordinates or parameters can be introduced into the neighborhood U. The problem consists in proving that every parameter group is a Lie group.

von Neumann (see [21]) solved this problem in the affirmative for compact groups by use of Theorem 28. For commutative groups the positive answer to this question was given by me (see Theorem 44).

On the basis of Theorem 28 results have been given after von Neumann's which expose the structure of compact topological groups and contain in particular the solution of Hilbert's problem (see [26], [14], and [16]). We devote the present chapter to the exposition of these results.

43. Approximation to Compact Groups by Lie Groups

We establish here on the basis of Theorem 28 certain connections between compact topological groups satisfying the second axiom of countability, and Lie groups. In particular we prove Theorem 54 which enables us to construct any compact group from Lie groups.

THEOREM 52. *Let Ω_n be the topological group of all unitary matrices of order n* (see §27, J)). *We denote by Ω the direct product of all the groups*

$\Omega_1, \Omega_2, \cdots, \Omega_n, \cdots$ (see Definition 29′). *Ω is a compact topological group satisfying the second axiom of countability. The theorem states that Ω is a universal group of all compact topological groups satisfying the second axiom of countability, i.e., every such group G is isomorphic with some subgroup of the group Ω.*

Proof. Let $g^{(1)}, g^{(2)}, \cdots, g^{(k)}, \cdots$ be the complete system of unitary representations of the group G, given in Theorem 28. We denote by p_k the degree of the representation $g^{(k)}$, and select an increasing sequence of natural numbers $n_1, n_2, \cdots, n_k, \cdots$ such that $p_k \leqq n_k$, $k = 1, 2, \cdots$. It follows from the last inequality that the totality of all unitary matrices of order p_k is a subgroup of Ω_{n_k}, and therefore the homomorphism $g^{(k)}$ can be considered as a homomorphism of the group G in the group Ω_{n_k}. From Definition 29′ every element of Ω represents a sequence $x = \{x_1, x_2, \cdots, x_n, \cdots\}$ such that $x_n \varepsilon \Omega_n$, $n = 1, 2, \cdots$. We now associate with every element $y \varepsilon G$ an element $f(y) = x \varepsilon \Omega$ defined by the following relations: $x_{n_k} = g^{(k)}(y)$, $k = 1, 2, \cdots$; if n is a natural number not belonging to the sequence n_k, then x_n is the identity of the group Ω_n. It can readily be seen that the mapping f thus obtained is a homomorphic mapping of the group G in the group Ω. We shall show that f is an isomorphic mapping of the group G on some subgroup G' of the group Ω.

Let $y \neq e$ be an element of the group G. Then by Theorem 28 there exists a number k such that $g^{(k)}(y) \neq e_{n_k}$ and therefore from the above construction of the mapping f, $f(y)$ is not the identity of the group Ω. In this way f is a one-to-one mapping. Since it is also continuous, it follows that $f(G) = G'$ is compact, and is therefore a closed subset of the space Ω (see Theorem 8, and §13, B)). Since G' is moreover an abstract group, Theorem 52 is proved.

We give one more direct corollary of Theorem 28.

Theorem 53. *Let G be a compact topological group satisfying the second axiom of countability, and U a neighborhood of the identity in G. Then there exists a normal subgroup $N \subset U$ of the group G such that the factor group G/N is a Lie group. We can even assert a little more, namely that there exists in G a decreasing sequence $N_1, N_2, \cdots, N_n, \cdots$ of normal subgroups such that their intersection contains only the identity and such that the factor group G/N_n is a Lie group for every n* (see Definition 38).

Proof. We denote by Φ_n the normal subgroup of the group Ω (see Theorem 52), defined as the product of the groups $\Omega_1, \cdots, \Omega_n$, and by Ψ_n the normal subgroup of the group Ω defined as the product of the groups $\Omega_{n+1}, \Omega_{n+2}, \cdots$. It can readily be seen that Ω is the direct product of the groups Φ_n and Ψ_n, and that the group Φ_n (see §20, G)) is isomorphic with the factor group Ω/Ψ_n. The group Φ_n is a Lie group, being the direct product of a finite number of Lie groups (see §38, C) and §41, A)). Hence Ω/Ψ_n is a Lie group. We note that the intersection of all the groups Ψ_n, $n = 1, 2, \cdots$, contains only the identity.

From Theorem 52 we can suppose that G is a subgroup of the group Ω. If we denote by N_n the intersection $G \cap \Psi_n$, then N_n is a normal subgroup of the

group G (see §20, C)). Under the homomorphism h_n of the group Ω on the group Ω/Ψ_n, the subgroup G goes into the subgroup G_n of the group Ω/Ψ_n, and since the group Ω/Ψ_n is a Lie group, its subgroup G_n is also a Lie group (see Theorem 50). But G_n is obviously isomorphic with G/N_n. Since, moreover, the intersection of all the groups Ψ_n contains only the identity, the intersection of all the groups N_n, $n = 1, 2, \cdots$, also contains only the identity.

Hence the groups N_n under consideration satisfy the conditions of the theorem. This proves Theorem 53.

DEFINITION 39. Let

$$(1) \qquad G_1, G_2, \cdots, G_n, \cdots$$

be a sequence of compact topological groups satisfying the second axiom of countability, and let g_n be a homomorphism of the group G_{n+1} on the group G_n, $n = 1, 2, \cdots$. We construct a compact topological group G from the sequence (1) and from

$$(2) \qquad g_1, g_2, \cdots, g_n, \cdots$$

This group G will satisfy the second axiom of countability, and we shall call it the *limit* of the sequence (1) under the homomorphisms (2).

We shall call a sequence

$$(3) \qquad x = \{x_1, x_2, \cdots, x_n, \cdots\}$$

fundamental if it is such that

$$(4) \qquad x_n \varepsilon G_n, \qquad n = 1, 2, \cdots,$$

and

$$(5) \qquad x_n = g_n(x_{n+1}), \qquad n = 1, 2, \cdots.$$

We denote the set of all fundamental sequences by G, and introduce into G a topology and a law of multiplication.

The *product* xy of two fundamental sequences $x = \{x_1, x_2, \cdots, x_n, \cdots\}$ and $y = \{y_1, y_2, \cdots, y_n, \cdots\}$ is defined by

$$xy = \{x_1y_1, x_2y_2, \cdots, x_ny_n, \cdots\}.$$

We introduce a topology into G by means of neighborhoods. A *neighborhood* U in G is defined by means of an arbitrary finite system of neighborhoods $U_1, \cdots, U_n$, where U_i is a neighborhood of the group G_i, $i = 1, \cdots, n$. Then U is composed of all the sequences (3) for which $x_i \varepsilon U_i$, $i = 1, \cdots, n$.

We first show that this really defines a compact topological group G satisfying the second axiom of countability.

We denote by Q the direct product of all the groups in the sequence (1). Then every fundamental sequence is an element of the group Q. Hence G is a subset of Q, $G \subset Q$. It can readily be seen that the law of multiplication and topology defined in G coincides with the law of multiplication and topology

induced in G from Q. We shall show that G is a subgroup of Q. In fact the element

(6) $$x = \{x_1, x_2, \cdots, x_n, \cdots\}$$

of the group Q belongs to G if and only if conditions (5) are satisfied for the sequence (6). It can be seen directly that every single equation $x_n = g_n(x_{n+1})$ singles out a subgroup P_n, while the totality of all conditions (5) corresponds to the intersection of all subgroups P_n, $n = 1, 2, \cdots$, i.e., it also singles out a subgroup (see §20, A)). Hence G is a compact topological group satisfying the second axiom of countability (see Definition 29′ and §17, B)). It can readily be seen that the limit of the sequence (1) remains unchanged if we discard a finite number of its initial members.

A) Let G be the limit of the sequence of groups (1) with the homomorphisms (2). We associate with every element $x \varepsilon G$ (see (3)) an element $h_n(x) = x_n \varepsilon G_n$. Then h_n is the homomorphism of the group G on the group G_n, where $h_n(x) = g_n(h_{n+1}(x))$. We denote the kernel of the homomorphism h_n by N_n. Then $N_{n+1} \subset N_n$, and the intersection of all the groups $N_1, N_2, \cdots, N_n, \cdots$ contains only the identity.

Proposition A) can be verified directly.

The construction introduced in Definition 39 can be justified by the following theorem.

THEOREM 54. *Every compact topological group G' which satisfies the second axiom of countability is isomorphic with the limit of some sequence of compact Lie groups* (see Definitions 38 and 39).

PROOF. Let $N_1, N_2, \cdots, N_n, \cdots$ be a decreasing sequence of normal subgroups of the group G', as was considered in Theorem 53. Let $G_n = G'/N_n$, and let h_n be the natural homomorphic mapping of the group G' on the group G_n. Since $N_{n+1} \subset N_n$, there exists one and only one homomorphic mapping g_n of the group G_{n+1} on the group G_n which is such that

(7) $$h_n(x') = g_n(h_{n+1}(x')).$$

The sequence of groups $G_1, G_2, \cdots, G_n, \cdots$ together with the homomorphisms $g_1, g_2, \cdots, g_n, \cdots$ has for its limit a group G. We shall show that G' is isomorphic with G. To do this we associate with every element $x' \varepsilon G'$ the element

(8) $$f(x') = \{h_1(x'), h_2(x'), \cdots, h_n(x'), \cdots\} = \{x_1, x_2, \cdots, x_n, \cdots\} = x$$

and show that the mapping f is an isomorphic mapping of the group G' on the group G.

It follows from (7) that the sequence (8) is fundamental, and therefore $f(x')$ is really an element of the group G. It can be verified directly that f is a homomorphic mapping of the group G' in the group G. We shall show that f is a mapping on the whole group G.

Let $a = \{a_1, a_2, \cdots, a_n, \cdots\}$ be an arbitrary element of the group G. We denote by A_n the set of all elements of the group G' which go into a_n under the homomorphism h_n. Since h_n is a mapping of the group G' on the whole group G_n, it follows that A_n is not empty. It is also obvious that A_n is compact. Furthermore, from relations (6) and (7) we have $A_{n+1} \subset A_n$. Hence the intersection of all the A_n, $n = 1, 2, \cdots$, is not empty (see Theorem 6), i.e., it contains at least one element a', and we have $h_n(a') = a_n$, $n = 1, 2, \cdots$, so that $f(a') = a$. Thus f is a mapping on the whole group G.

We shall now show that f is an isomorphic mapping.

If $f(x')$ is the identity, then $h_n(x')$ is the identity of the group G_n and therefore $x' \varepsilon N_n$, $n = 1, 2, \cdots$. Since the intersection of all N_n, $n = 1, 2, \cdots$, contains only the identity, the kernel of the homomorphism f contains only the identity, and therefore the homomorphism f is an isomorphism (see Theorem 13, and §19, D)).

Since all the groups G_n are Lie groups (see Theorem 53), Theorem 54 is proved.

Example 57. Let D be the additive topological group of real numbers and let N be the subgroup of all integers. We let $K = D/N$, and denote by G_n, $n = 1, 2, \cdots$, a sequence of groups isomorphic with K; $G_n = f_n(K)$, where f_n is an isomorphic mapping. Then there exists an inverse mapping f_n^{-1} which is also isomorphic. We now define the homomorphism g_n of the group G_{n+1} on the group G_n by letting $g_n(x) = f_n(s_n f_{n+1}^{-1}(x))$, where $x \varepsilon G_{n+1}$, and s_n is an arbitrary integer which defines the homomorphism g_n. The sequence of groups $G_1, G_2, \cdots, G_n, \cdots$ together with the homomorphisms $g_1, g_2, \cdots, g_n, \cdots$ defines a group G (see Definition 39). This group G depends on the choice of the numbers s_n, $n = 1, 2, \cdots$. If these numbers beginning with a certain number are all equal to unity, then G is isomorphic with K. Otherwise, the group G has a rather complicated structure. This structure will be clarified in the sections that follow.

We note also that the set of all possible groups G obtained for different choices of s_n coincides with the set of all groups X given in example 53.

Example 58. Let

$$G_1, G_2, \cdots, G_n, \cdots \tag{9}$$

be a sequence of finite groups and $g_1, g_2, \cdots, g_n, \cdots$ a sequence of homomorphisms, where g_n is a homomorphism of the group G_{n+1} on the group G_n. Then the limit of the sequence (9) is a 0-dimensional group (see Definition 39).

In fact let N_n be the normal subgroup of the group G defined in remark A). Then the factor group G/N_n is finite, and therefore the set containing only its identity is an open set, and hence N_n, being a complete inverse image of this open set in the group G, is itself an open set in G. Since by A) there exists an arbitrarily small subgroup of the type N_n, the group G is 0-dimensional (see §22, C)).

Conversely, every 0-dimensional compact topological group can be obtained as a limit of a sequence of finite groups (see §22, E)).

44. Auxiliary Topological Concepts

We define in this section two auxiliary topological concepts: dimension and local connectedness. They will be used in the near future in order to impose further restrictions on general topological groups.

A) Let R be a compact regular topological space satisfying the second axiom of countability (see Definitions 19, 17, and 18). We shall say that there exists a *finite covering* Ω *of the space* R *by open sets* if there exists a finite system $\Omega = \{U_1, \cdots, U_n\}$ of open sets whose sum contains R. Analogously we shall say that there exists a *finite covering* Δ *of the space* R *by closed sets* if there exists a finite system $\Delta = \{F_1, \cdots, F_m\}$ of closed sets whose sum contains R. If for every $F_i \varepsilon \Delta$ there exists an open set $U_j \varepsilon \Omega$ such that $F_i \subset U_j$, we shall say that Δ is a *refinement* of Ω and write $\Delta \Subset \Omega$. We shall say that the covering Δ has the *multiplicity* k if the system Δ has at most k sets having a common point.

Using the above terminology, we give a definition of the dimension of a space.

Definition 40. A compact regular space R has a *finite dimension* r if the following conditions are satisfied:

1) For every finite covering Ω of the space R by open sets, there exists a finite covering Δ of the space R by closed sets such that $\Delta \Subset \Omega$ and the multiplicity of the covering Δ does not exceed $r + 1$ (see A)).

2) There exists a finite covering Ω of the space R by open sets such that if Δ is a covering of the space R by closed sets which is a refinement of Ω, then the multiplicity of Δ exceeds r.

In case there exists no r satisfying the above conditions, we say the dimension of the space R is *infinite.*

The above definition of dimension is justified in the first place by the following proposition B), whose proof is not given because of its complexity.

B) If R is a cube of an n-dimensional Euclidean space, then the dimension of the space R (see Definition 40) is equal to n (see [2] and [3]).

I give here without proof another property of the concept of dimension.

C) If the space R decomposes into a sum of a finite number of closed subsets $R_1, \cdots, R_k$, then the dimension of the space R is equal to the maximum of the dimensions of the spaces R_i, $i = 1, \cdots, k$.

In considering the dimension of the space of a topological group, we can restate the definition of dimension in a way better suited to our purposes.

D) Let G be a compact topological group satisfying the second axiom of countability, and V a neighborhood of the identity in the group G. We shall say that the finite covering $\Delta = \{F_1, \cdots, F_m\}$ of the space G by closed sets is a *V-covering* if $F_iF_i^{-1} \subset V$, $i = 1, \cdots, m$. Then the dimension r of the space G is defined by the following conditions:

a) For every neighborhood V of the identity of the group G there exists a finite V-covering of the space G by closed sets whose multiplicity does not exceed $r + 1$.

b) There exists a neighborhood V of the identity of the group G such that every finite V-covering of the space G by closed sets has a multiplicity greater than r.

In case there exists no finite number r satisfying conditions a) and b), the dimension of the space G is said to be infinite.

We proceed to prove proposition D).

We suppose that the dimension of the space G is equal to r, and show that for every neighborhood V of the identity there exists a V-covering of multiplicity $\leqq r + 1$.

Let W be a neighborhood of the identity such that $WW^{-1} \subset V$. The set of all regions Wx, where $x \in G$, covers the group G; hence by Theorem 7 we can select from this covering a finite covering $\Omega = \{Wa_1, \cdots, Wa_n\}$. Since the dimension of the space G is equal to r by assumption, there exists a finite covering $\Delta = \{F_1, \cdots, F_m\}$ of the space G by closed sets such that $\Delta \Subset \Omega$, and such that its multiplicity does not exceed $r + 1$. Since every F_i is contained in some region Wa_j, it follows that $F_iF_i^{-1} \subset WW^{-1} \subset V$. Hence Δ is a V-covering whose multiplicity does not exceed $r + 1$.

Let us now suppose that the dimension of G is r, where r may be infinite. We then show that for every finite $s \leqq r$ there exists a neighborhood V of the identity such that every V-covering of the space G has a multiplicity which exceeds s. The case of $s < r$ is only of interest for $r = \infty$.

Let $\Omega = \{U_1, \cdots, U_n\}$ be a finite covering of the space G by open sets such that every covering Δ which is a refinement of Ω has a multiplicity which is greater than s (see Definition 40). For every point $x \in G$ there exists a number k such that $x \in U_k$. We denote by V_x a neighborhood of the point x such that $\overline{V}_x \subset U_k$. We select from the covering of the space G by open sets V_x the finite covering

$$(1) \qquad V_{x_1}, \cdots, V_{x_p}.$$

The covering (1) possesses the property that for every open set V_{x_i} there exists an open set U_j such that $V_{x_i} \subset U_j$. Let $E_j = G - U_j$. The set $E_jV_{x_i}^{-1}$ is a compact set which does not contain the identity, and therefore there exists a neighborhood of the identity V which does not intersect any of the sets $E_jV_{x_i}^{-1}$. Suppose now that there exists a finite V-covering $\Delta = \{F_1, \cdots, F_m\}$ by closed sets whose multiplicity is s. We shall show that this is impossible; in fact we shall show that $\Delta \Subset \Omega$.

Since (1) forms a covering of the space G, there exists for every F_k a number i such that F_k and V_{x_i} intersect. It can readily be seen that in this case F_k cannot intersect E_j, since $E_jV_{x_i}^{-1}$ does not intersect V, and $F_kF_k^{-1} \subset V$. Hence $F_k \subset U_j$, i.e., $\Delta \Subset \Omega$, and therefore by assumption the dimension of the covering Δ exceeds s.

Hence proposition D) is completely proved.

E) Let G be a compact topological group satisfying the second axiom of countability. If the group G is 0-dimensional (see §22, B)), it is of dimension zero (see Definition 40) and conversely if the group G is of dimension zero, then it is 0-dimensional.

Let V be an arbitrary neighborhood of the identity in the group G. If the group G is 0-dimensional, then there exists an open normal subgroup N such that $N \subset V$ (see §22, E)). We denote by

$$A_1, \cdots, A_m \tag{2}$$

the cosets of G by the normal subgroup N. From remark E) of §22 there are just a finite number of such cosets. It can readily be seen that the system of sets (2) forms a finite V-covering of the space G by closed sets, having the multiplicity one. Hence the dimension of the space G is zero.

Let us now suppose, conversely, that G is of dimension zero. Suppose that G contains a connected closed set S, containing the identity and an element $a \neq e$. We shall show that this is impossible.

Let V be a neighborhood of the identity in the group G which does not contain the element a. Since the dimension of G is zero, there exists a finite V-covering Δ of the space G by closed non-intersecting sets. We denote by F that set of the system Δ which contains e, and by E the sum of all the other sets of the system. Let $A = S \cap F$, and $B = S \cap E$. It can readily be seen that the sets A and B are not empty and do not intersect; further, they are closed. Hence S is not connected and we have arrived at a contradiction. This proves E).

F) Let G be a compact topological group satisfying the second axiom of countability and of dimension $r \leqq \infty$. Let s be a finite number not exceeding r. Then there exists a neighborhood U of the identity such that if a normal subgroup N of the group G is in U, then the factor group G/N is of dimension not less than s.

We denote by V a neighborhood of the identity of the group G such that every finite V-covering of the space G by closed sets has a multiplicity which exceeds s. Let U, furthermore, be a neighborhood of the identity of the group G such that $U^2 \subset V$. Suppose that N is a normal subgroup of the group G contained in U, $N \subset U$, and let $G/N = G'$. We denote by g the natural homomorphic mapping of the group G on the group G'. Let $g(U) = U'$. It is easy to see that the complete inverse image $g^{-1}(U')$ of the set U' under the mapping g is contained in V, $g^{-1}(U') \subset V$.

Suppose the dimension of the group G' does not exceed $s - 1$; we shall show that this is impossible.

Let $\Delta' = \{F_1', \cdots, F_m'\}$ be a finite U'-covering of the space G' by closed sets whose multiplicity does not exceed s (see D)). We denote by F_i the complete inverse image in G of the set F_i'. It can readily be seen that $\Delta = \{F_1, \cdots, F_m\}$ is a finite V-covering of the space G by closed sets whose multiplicity is equal to

the multiplicity of the covering Δ'. But this contradicts our original assumption about V. This proves F).

G) Let G be a compact Lie group of dimension r (see Definition 38). Then the dimension of the group G, in the sense of Definition 40, is also r.

Since G has the dimension r in the sense of Definition 38, there exists a neighborhood U of the identity of the group G such that $\overline{U}$ is homeomorphic with an r-dimensional cube. The whole group G can easily be represented as the sum of a finite number of subsets of the form $\overline{U}x$. In this way by remarks B) and C) the dimension of the space G is r in the sense of Definition 40 as well.

DEFINITION 41. Let R be a compact regular topological space satisfying the second axiom of countability. The space R is called *locally connected* if for every point a and neighborhood U of a there exists a neighborhood $V \subset U$ of a such that for every $x \in V$, U contains a connected set containing both a and x.

H) It can readily be seen that every compact Lie group is locally connected.

45. Compact Topological Groups of Finite Dimension

We investigate in this section compact topological groups satisfying the second axiom of countability which have a finite dimension. A positive solution of Hilbert's fifth problem will be given here for compact groups on the basis of this investigation (see Theorem 57).

A) Let G and H be two Lie groups (see Definition 38) and let f be a homomorphic mapping of the group H on the group G. Furthermore let $x(t)$, $|t| \leqq \alpha$, be a one-parameter subgroup defined in G (see §39, A)). Then H contains a one-parameter subgroup $y(t)$, $|t| \leqq \alpha$, such that $f(y(t)) = x(t)$ for $|t| \leqq \alpha$.

To prove this, we introduce canonical coordinates of the first kind in the neighborhoods of the identities of the groups G and H (see §39, B)). Then the mapping f will be expressed in the neighborhood of the identity in the form of a linear mapping (see §42, B)). It follows from this that H contains a one-parameter subgroup $y'(t)$ defined for small values of the parameter such that $f(y'(t)) = x(t)$. Extending this subgroup to values of the parameter $|t| \leqq \alpha$ we obtain the desired group $y(t)$, $|t| \leqq \alpha$.

B) Let G be the topological group which is the limit of the sequence of compact Lie groups $G_1, G_2, \cdots, G_n, \cdots$ having $g_1, g_2, \cdots, g_n, \cdots$ for homomorphisms (see Definition 39). Furthermore let $x_1(t)$, $|t| \leqq \alpha$, be a one-parameter subgroup defined in G, and let h_1 be the homomorphic mapping of the group G on the group G_1 discussed in remark A), §43. Then G contains a one-parameter subgroup $x(t)$, $|t| \leqq \alpha$, such that

$$(1) \qquad h_1(x(t)) = x_1(t) \quad \text{for} \quad |t| \leqq \alpha.$$

By remark A), G_2 contains only one one-parameter subgroup $x_2(t)$, $|t| \leqq \alpha$, such that $g_1(x_2(t)) = x_1(t)$ for $|t| \leqq \alpha$. Continuing this process of construction we obtain an infinite sequence of one-parameter subgroups $x_1(t), x_2(t), \cdots, x_n(t), \cdots$ where $x_n(t)$, $|t| \leqq \alpha$, is a one-parameter subgroup

of the group G_n, while $g_n(x_{n+1}(t)) = x_n(t)$ for $|t| \leqq \alpha$ and $n = 1, 2, \cdots$. Let $x(t) = \{x_1(t), x_2(t), \cdots, x_n(t), \cdots\}$ (see Definition 39). Then $x(t)$ is an element of the group G which depends on the parameter t, and is defined for all values of t which are less than α in absolute value. It can readily be seen that $x(t)$ is a one-parameter subgroup in G which satisfies condition (1).

THEOREM 55. *Let G be a compact topological group of finite dimension r satisfying the second axiom of countability. Then G contains a local Lie subgroup L of dimension r* (see Definition 38 and §23, I)), *and a 0-dimensional normal subgroup Z* (see §22, B)) *such that $U = LZ$ is a neighborhood of the identity in G, and U decomposes into the direct product of the local subgroup L and the normal subgroup Z* (see §23, L)). *In case G is connected, Z is a central normal subgroup of the group G* (see §22, D)).

In greater detail: every element $u \varepsilon U$ is decomposed uniquely and continuously into the product

$$u = lz, \quad \text{where} \quad l \varepsilon L, z \varepsilon Z, \tag{2}$$

and $lz = zl$. The continuity of the decomposition (2) *means that the elements $l = l(u)$ and $z = z(u)$, which are defined uniquely by* (2), *are continuous functions of the element u.*

PROOF. It follows from Theorem 54 that G may be considered as the limit of a sequence of compact Lie groups

$$G_1, G_2, \cdots, G_n, \cdots \tag{3}$$

with homomorphisms

$$g_1, g_2, \cdots, g_n, \cdots. \tag{4}$$

We introduce into the group G_1 canonical coordinates D of the second kind (see §40, A)), constructing them on the basis of the one-parameter subgroups

$$x_1'(t), \cdots, x_s'(t), \qquad |t| \leqq \alpha.$$

We denote by L_β' the set of all points of the form

$$x' = x_1'(t^1) \cdots x_s'(t^s), \qquad |t^k| < \beta, \qquad k = 1, \cdots, s, \beta \leqq \alpha.$$

Let α be a positive number sufficiently small to insure that L_α' is a region of existence of the coordinates D. Let h_1 be the homomorphic mapping of the group G on the group G_1 introduced in remark A) of §43. Then it follows from B) that G contains a one-parameter subgroup $x_i(t)$, $|t| \leqq \alpha$, such that $h_1(x_i(t)) = x_i'(t)$ for $|t| \leqq \alpha$, $i = 1, \cdots, s$. We denote by L_β the set of all elements of the form

$$x = x_1(t^1) \cdots x_s(t^s), \qquad |t^k| < \beta \qquad k = 1, \cdots, s, \beta \leqq \alpha.$$

Obviously $h_1(x) = x'$. We shall show that the mapping h_1 is topological on the set L_α.

To every element x' corresponds uniquely an element x. Hence the mapping h_1 of the set L_α on the set L'_α has a unique inverse mapping and therefore the mapping h_1 itself is one-to-one on the set L_α. Furthermore, we have $\overline{L}_\beta \subset L_\alpha$ for $\beta < \alpha$, and since $\overline{L}_\beta$ is compact, the mapping h_1, being continuous and one-to-one, is topological on $\overline{L}_\beta$ (see Theorem 8), and this implies that h_1 is topological on the whole set L_α.

Hence we see that G contains an s-dimensional cube $\overline{L}_\beta$, and therefore the dimension of the group G is not less than s (see §44, C)). Therefore $s \leqq r$. Since it is possible to omit a finite number of members of the sequence (3) without changing the limit G, it follows that the dimension of every group of the sequence (3) does not exceed r.

We shall show that the dimension of every group G_n of (3) after a certain n is equal to r.

There exists a neighborhood V of the identity of the group G such that if $N \subset V$ is a normal subgroup of the group G, then the dimension of G/N is not less than r (see §44, F)). By remark A) of §43, the group G_n is isomorphic with the factor group G/N_n, where $N_{n+1} \subset N_n$, and the intersection of the groups $N_1, N_2, \cdots, N_n, \cdots$ contains only the identity. Hence after a certain n, $N_n \subset V$, i.e., the dimension of the group G_n is not less than r. Therefore, after a certain n the dimension of the groups G_n in the sequence (3) is equal to r.

We shall therefore say that all the groups of the sequence (3) are of dimension r since the omission of the first few members of this sequence does not change the limit G. In particular the local Lie group L'_β is of dimension r, $s = r$.

We denote by Z the kernel of the homomorphism h_1, and show that Z is a 0-dimensional group, and that if G is connected, then Z belongs to the center.

We denote by Z_2 the totality of all the elements of the group G_2 which go into the identity under the homomorphism g_1, and by Z_3 the totality of all the elements which go into Z_2 under the homomorphism g_2, and, in general, by Z_{n+1} the totality of all the elements which go into Z_n under the homomorphism g_n. Since the dimension of all the groups in (3) is r, and since Z_n is the kernel of the homomorphism of the group G_n on G_1 obtained through the homomorphisms $g_{n-1}, \cdots, g_2, g_1$, it follows that Z_n has dimension zero (see Theorem 51) and therefore all the groups Z_n are finite, being compact Lie groups of dimension zero (see Theorem 50). We also note that Z_n is a normal subgroup of the group G_n (see Theorem 12) and hence Z_n belongs to the center if it is connected (see Theorem 16). But if G is connected, G_n is also connected, since G_n is a homomorphic image of the group G (see §43, A)). Hence Z_n belongs to the center if G is connected. It is not hard to see that the groups $Z_2, Z_3, \cdots, Z_n, \cdots$ with homomorphisms $g_2, g_3, \cdots, g_n, \cdots$ have as their limit the group Z, and therefore Z is 0-dimensional (see Example 58). In case G is connected Z belongs to the center, since, as is easy to verify, the limit of a sequence of central normal subgroups is itself a central normal subgroup.

We denote by U_β the complete inverse image of the neighborhood L'_β under

the homomorphism h_1. Then U_β is a neighborhood of the identity in G. We shall show that $U_\beta = L_\beta Z$, where every element $u \varepsilon U_\beta$ decomposes uniquely into the product

$$(5) \qquad u = lz, \qquad l \varepsilon L_\beta, \qquad z \varepsilon Z.$$

If $u \varepsilon U_\beta$, then $h_1(u) \varepsilon L'_\beta$ and therefore there exists an element $l \varepsilon L_\beta$ such that $h_1(u) = h_1(l)$. Then we have $h_1(l^{-1}u) = e$, i.e., $l^{-1}u = z \varepsilon Z$. Hence $u = lz$. If, moreover, $u = l'z'$ with $l' \varepsilon L_\beta$ and $z' \varepsilon Z$, then $h_1(u) = h_1(l) = h_1(l')$, and hence $l = l'$, since the mapping h_1 is one-to-one on L_β. Hence $l' = l$, $z' = z$ and the decomposition (5) is established.

We shall now show that the decomposition (5) is continuous, i.e., the elements $l = l(u)$ and $z = z(u)$ are defined uniquely by (5) and are continuous functions of the element u.

For $\beta < \alpha$ we have $\bar{U}_\beta \subset U_\alpha$ and therefore the decomposition (5) is unique for all elements of the set $\bar{U}_\beta$. In this way the set $\bar{U}_\beta$ is a unique and continuous image of the topological product of the spaces $\bar{L}_\beta$ and Z (see Definition 21). Since this topological product is compact (see §15, E)), it follows that $\bar{U}_\beta$ is simply homeomorphic to the topological product of the spaces $\bar{L}_\beta$ and Z (see Theorem 8). This proves the continuity of the decomposition (5).

We shall show next that for a sufficiently small γ, $L_\gamma = L$ is a local Lie group, and h_1 is an isomorphic mapping of the local Lie group L_γ on the local group L'_γ.

Since the mapping h_1 is homeomorphic and homomorphic on L_β, it is sufficient to select $\gamma \leqq \beta$ in such a way that for $a \varepsilon L_\gamma$, $b \varepsilon L_\gamma$, and $ab \varepsilon U_\gamma$ we have $ab \varepsilon L_\gamma$. Let γ be sufficiently small so that $L_\gamma^2 \subset U_\beta$. Then the function $z(u)$ is defined on L'_γ. Since $z(L_\gamma^2) \subset Z$ is connected and contains the identity, and since Z is 0-dimensional, it follows that $Z(L_\gamma^2) = \{e\}$, i.e., $ab \varepsilon L_\gamma$.

We shall finally show that every element of the group Z commutes with every element of the group L_γ.

Let $z \varepsilon Z$. We are to show that $lzl^{-1} = z$ for $l \varepsilon L_\gamma$. We shall move l continuously in the interior of L_γ towards the identity. Since Z is a normal subgroup, lzl^{-1} always belongs to Z, and therefore describes a continuous curve in Z. Since Z is 0-dimensional, we have $lzl^{-1} = z$. Hence Theorem 55 is completely established.

Theorem 56. *Let G be a compact topological group satisfying the second axiom of countability. If G is locally connected* (see Definition 41) *and is of finite dimension, it is a Lie group.*

Proof. Let U be the neighborhood of the identity defined in Theorem 55. If Z is a finite group, then L is a neighborhood in G, and since L is a local Lie group, G is also a Lie group. We shall show that in case the group Z is infinite, G is not locally connected.

Suppose that G is locally connected. Then there exists a neighborhood $V \subset U$ of the identity e of the group G such that if $x \varepsilon V$, then there exists a connected set $S \subset U$ which contains both x and e. Since Z is infinite by as-

sumption, and is also compact, there exists a point $x \in Z \cap V$ distinct from the identity. Let $S \subset U$ be a connected set containing the points x and e. We associate with every point $u = lz \in S$, where $l \in L$ and $z \in Z$, a point $z = z(u)$. The mapping $z(u)$ is continuous, and therefore the set $z(S)$ is a connected set containing the points e and x. But this is impossible since Z is 0-dimensional and $z(S) \subset Z$, while $x \neq e$. This proves Theorem 56.

As a consequence of Theorem 56 we prove the following proposition.

Theorem 57. *Let G be a compact topological group satisfying the second axiom of countability. If there exists a neighborhood V of the identity of the group G which is homeomorphic with a Euclidean space then G is a Lie group.*

Proof. It follows from the fact that the neighborhood V is homeomorphic with the Euclidean space that G is of finite dimension and is locally connected. Hence G is a Lie group by Theorem 56.

Example 59. Let G be a connected compact topological group of finite dimension satisfying the second axiom of countability, and let L be a local Lie group of the sort defined in Theorem 55. We denote by G' the set of all the elements of G which can be represented in the form of finite products of elements belonging to L. Then G' is a subgroup of the abstract group G. It is not hard to see that G' is a homomorphic image of some Lie group G^*, i.e., $G' = f(G^*)$, where f is a one-to-one mapping, which, however, is continuous in one direction only. Moreover it turns out that the set G' is everywhere dense in G.

CHAPTER VIII

LOCALLY ISOMORPHIC GROUPS

We shall develop in this chapter the results of Schreier (see [31] and [32]) concerning the connection in the large between locally isomorphic groups (see Definition 30). We have already considered this question in Theorem 18. Here we shall obtain deeper results by narrowing down the class of groups under consideration. It will be shown that from the totality of all groups locally isomorphic with a given group G a certain group G^*, which is called the universal covering group, is naturally singled out. Moreover, every group which is locally isomorphic with the group G^* can be obtained as a factor group G^*/N, where N is a discrete normal subgroup of the group G^*. The construction of a universal covering group is based on a process applicable not only to topological groups, but to a wider class of topological spaces. In the construction of a universal covering group we run across the important topological concept, due to Poincaré, of the fundamental group.

One should not think that Schreier's results reduce completely the study of a topological group to its local properties. His results only give a method of constructing all groups locally isomorphic with a given group. The study of the properties of this given group, however, cannot be reduced to the study of its local properties. We shall meet this sitation in the next chapter.

It should be noted that the results of this chapter belong to Schreier only in the sense that he has organized and formulated them. The concepts which we shall discuss here have been used independently by Weyl (see [35]) and others.

46. Fundamental Group. Covering Space

We shall consider here some purely topological concepts which, because of their generality, we shall not restrict to topological groups.

A) We say that the topological space R contains a *path* or a *curve* l if in it is defined a function $f(t)$ of a real parameter t, $0 \leqq t \leqq 1$, which associates with every number t, $0 \leqq t \leqq 1$, a definite point $f(t)$ in the space R. The point $f(0)$ is called the *beginning* of the path l, and the point $f(1)$, its *end*. The path l *connects* the points 0 and 1 in the space R. The path l is called a *null* or *identity path* if the function $f(t)$ is a constant. Let the *opposite* or *inverse* path to the given path l, denoted by l^{-1}, be given by the function $f(1 - t)$ of the parameter t. If two paths k and l are given by the functions $f(t)$ and $g(t)$ such that the end of the first path coincides with the beginning of the second path, i.e., $f(1) = g(0)$, then we can define the *product* kl of the paths k and l as follows. The product kl is defined by the function $h(t)$ which is defined by $h(t) = f(2t)$ for $0 \leqq t \leqq \frac{1}{2}$, and $h(t) = g(2t - 1)$ for $\frac{1}{2} \leqq t \leqq 1$. Let l be called *closed* if its beginning and end coincide.

One should not think that the totality of all paths given in the space G forms a group. First, multiplication is not always possible. Moreover, the product does not satisfy the associative law, and the product of the path l by its inverse l^{-1} is not a null path; nor is the product of the path l by a null path the path l, but rather something new. Because of this the paths themselves will not interest us a great deal. What will be important for our purposes are the classes of equivalent or homotopic paths. Certain totalities of these classes also form a group, namely the fundamental group.

B) Two paths k and l in the space R are called *homotopic* or *equivalent*, denoted by $k \sim l$, if there exists a continuous deformation of the path k which does not displace the beginning and end points of k and changes k into l. This definition can be expressed more fully as follows: Let $f(t)$ and $g(t)$ be the functions which define the paths k and l. The paths k and l are called equivalent if there exists a function $\varphi(s, t)$, continuous simultaneously in both its real parameters s and t, $0 \leqq t \leqq 1$, $0 \leqq s \leqq 1$, and such that $\varphi(0, t) = f(t)$, $\varphi(1, t) = g(t)$, $\varphi(s, 0) = f(0) = g(0)$, $\varphi(s, 1) = f(1) = g(1)$.

A closed path l is called *homotopic* or *equivalent to zero*, $l \sim 0$, if the path l is equivalent to a null path.

It is not difficult to see that the concept of equivalence which we have introduced here is reflexive, i.e., $l \sim l$, symmetric, i.e., if $k \sim l$, then $l \sim k$, and transitive, i.e., if $k \sim l$, and $l \sim m$, then $k \sim m$. It is also not hard to see that if $k \sim k'$ and $l \sim l'$, and if the product kl is defined, then the product $k'l'$ is also defined and

$$k'l' \sim kl; \tag{1}$$

moreover

$$k^{-1} \sim k'^{-1}. \tag{1'}$$

C) Let k be an arbitrary path, l a null path, and let the product kl be defined. Then $kl \sim k$.

This proposition is obvious but I shall give here a formal proof.

Let $f(t)$ be the function which defines the path k. We define the function $\varphi(s, t)$ as follows; $\varphi(s, t) = f(2t/(1 + s))$ for $0 \leqq t \leqq (1 + s)/2$, and $\varphi(s, t) = f(1)$ for $(1 + s)/2 \leqq t \leqq 1$. It can be checked readily that the function $\varphi(s, t)$ defines a continuous deformation of the path kl into the path k (see B)). Hence $kl \sim k$.

D) If k, l, and m are three paths such that the products kl and lm are defined, then $(kl)m \sim k(lm)$.

To prove this let $f(t)$, $g(t)$, and $h(t)$ be the three functions which define the paths k, l, and m. Then the function $\varphi(s, t)$ is defined as follows;

$$\begin{aligned}
\varphi(s, t) &= f(4t/(1 + s)), && \text{for } 0 \leqq t \leqq (1 + s)/4 \\
\varphi(s, t) &= g(4t - 1 - s), && \text{for } (1 + s)/4 \leqq t \leqq (2 + s)/4 \\
\varphi(s, t) &= h(1 - 4(1 - t)/(2 - s)), && \text{for } (2 + s)/4 \leqq t \leqq 1.
\end{aligned}$$

It can readily be verified that the function $\varphi(s, t)$ performs the continuous deformation of the path $(kl)m$ into the path $k(lm)$.

E) Let k and l be two paths such that the product kl^{-1} exists and the path kl^{-1} is closed. Then the relations

$$k \sim l \tag{2}$$

and

$$kl^{-1} \sim 0 \tag{3}$$

follow one from the other.

We shall show first that (3) follows from (2). First, since $k \sim l$, it follows from (1) that $kl^{-1} \sim ll^{-1}$ and it is sufficient to show that $ll^{-1} \sim 0$. Let $g(t)$ be the function which defines l. The function $\varphi(s, t)$ we define as follows: $\varphi(s, t) = g(2t(1 - s))$, for $0 \leqq t \leqq 1/2$, and $\varphi(s, t) = g(2(1 - t)(1 - s))$ for $1/2 \leqq t \leqq 1$. It can readily be checked that the function $\varphi(s, t)$ performs the deformation of the path ll^{-1} into a null path.

Suppose now that (3) holds. This means that there exists a function $\psi(s, t)$ which deforms the path kl^{-1} into a null path. Denoting by $f(t)$ the function which defines the curve k, we have $\psi(0, 1) = f(2t)$ for $0 \leqq t \leqq 1/2$, and $\psi(0, t) = g(2 - 2t)$ for $1/2 \leqq t \leqq 1$. Furthermore $\psi(s, 0) = \psi(1, t) = \psi(s, 1) = f(0) = g(0)$.

We shall give a geometric interpretation of these equations. We shall consider a square Q in the plane s, t, which is defined by the inequalities: $0 \leqq s \leqq 1$, $0 \leqq t \leqq 1$. The function $\psi(s, t)$ gives a continuous mapping of this square on the space R under consideration. Under this mapping, as is clear from the above relations, three sides of the square Q go into one point $f(0) = g(0)$, namely the sides

$$(0, 0) - (1, 0); \qquad (1, 0) - (1, 1); \qquad (1, 1) - (0, 1).$$

The remaining side $(0, 0) - (0, 1)$ goes into the curve kl^{-1}, or more exactly, its segment $(0, 0) - (0, 1/2)$ goes into k, while the segment $(0, 1) - (0, 1/2)$ goes into l. Geometrically it is obvious that inside the square Q it is possible by means of a continuous deformation to change the segment $(0, 0) - (0, 1/2)$ into the segment $(0, 1) - (0, 1/2)$ so that the vertex $(0, 1/2)$ remains stationary, while the vertex $(0, 0)$ moves along the sides of the square which map into the point $f(0) = g(0)$. It is clear that if we map this deformation by means of the function $\psi(s, t)$ in R we get the deformation of the path k into the path l. This proves E).

F) In this chapter we shall call a topological space *connected* if any two of its points can be joined by a curve (see A)).

Definition 42. Let R be a connected topological space (see F)) and p one of its points. We denote by P the totality of closed paths in R which begin at p. We divide the set P into classes, putting in each class all the paths which are equivalent (see B)). The set of all the classes thus obtained we denote

by G, and we define the group operation in G as follows: Let A and B be two elements of the set G. We denote by a a path of the class A, and by b a path of the class B. The paths a and b can be multiplied (see A)), since they begin and end in p. Let $c = ab$. We denote by C that class of paths which contains c. It follows from (1) that the class C is uniquely defined by the classes A and B. We define the product AB by setting $AB = C$. The group G thus obtained does not depend on the choice of the point p, is a topological invariant of the space R, and is called the *fundamental group* of this space.

It is not hard to see that the operation of multiplication which we have defined in G satisfies all the conditions of Definition 1. The associativity follows from D). The identity of the group G is the class composed of all the paths of the set P which are homotopic to zero (see C)). Finally if A is an element of the set G, then A^{-1} is defined as the class composed of all the paths opposite to the paths of class A (see (1′) and E)).

We shall now show that the fundamental group G of the space R does not depend on the choice of the point p. Let p' be another point, and let G' be the fundamental group constructed on the basis of the point p' in the same way as G was constructed from p. We shall show that G and G' are isomorphic.

Let l be a path from the point p' to the point p; such a path exists since R is connected by assumption (see F)). Let A be an arbitrary element of the group G, and a a path of class A. Let $a' = lal^{-1}$, and let A' be the class containing a'. It follows from (1) and (1′) that the class A' is uniquely determined by the class A, i.e., it does not depend on the choice of the path a of the class A (of course, it is supposed that l is fixed). Let $A' = \varphi(A)$. We can then show that φ is an isomorphic mapping of the group G on the group G'. We show first of all that the mapping φ is one-to-one. To do this consider the path $l^{-1}a'l$. It is not hard to see that the path $l^{-1}a'l = l^{-1}lal^{-1}l$ is homotopic to the path a (see C), E) and (1), (1′)). Hence the class A in turn is uniquely defined by the class A' and the mapping φ is one-to-one. Because of the complete symmetry of the roles played in this investigation by G and G', the mapping φ is a mapping on the whole group G'. It can readily be shown that φ preserves the law of multiplication. In fact let A and B be two elements of the set G, and let a be a path in A and b a path in the class B. Let $a' = lal^{-1}$, $b' = lbl^{-1}$, $c = ab$. It follows from C), E), and (1) that the paths $a'b'$ and lcl^{-1} are equivalent, and this means that $\varphi(AB) = \varphi(A)\varphi(B)$. Hence the isomorphism between the group G and G' is established.

We should note that the isomorphic mapping φ which we have just constructed depends on the choice of the path l. Hence φ is not defined uniquely. In particular if the points p and p' coincide, then our construction can still be carried out, if we take for l some closed path which begins and ends in the point p. The isomorphism p thus obtained will be an automorphism of the group G, and can easily be shown to be an inner automorphism (see §3, B)).

G) A connected space R is called *simply connected* if its fundamental group

contains only the identity. This condition expresses the fact that every closed path defined in R is homotopic to zero.

H) A space R is called *locally simply connected,* if for every point p and neighborhood U of p there exists a neighborhood $V \subset U$ of the same point such that any closed curve beginning at p, and contained in V is homotopic to zero in U.

I) We shall call a space R *locally connected* in this chapter if for every point p and neighborhood U of p there exists a neighborhood $V \subset U$ of the same point p such that for $x \in V$ there exists a curve in U which connects the points p and x.

It can readily be seen that from the above definition of local connectedness, and from the condition of connectedness in the sense of Definition A) of §11 follows connectedness in the sense of Definition F). We shall not make use of this fact, however.

Definition 43. Let R be a connected, locally connected, locally simply connected space, and let p be one of its points (see F), I), and H)). Let Q be the set of all the paths of the space R which begin at p. We divide the set Q into classes, putting in each class the totality of all equivalent paths, We denote the set of classes thus obtained by S. We note that there exists a natural mapping φ of the set S on the space R. In fact if $A \in S$, then all the paths which belong to the class A end in the same point a, and we write $a = \varphi(A)$. We now introduce a topology into S, by defining an arbitrary neighborhood U^* of the topological space S in terms of a certain neighborhood U of the space R and a certain path $l \in Q$, which ends in U. Let x be an arbitrary path in U whose beginning coincides with the end of the path l. Let $y = lx$, and let Y be the totality of all the paths equivalent to the path y. We denote by U^* the set of all classes Y obtained from all possible choices of x in U. It is not hard to see that the set U^* will not change if the path l is replaced by the path $l' \in A$, where $A \in U^*$. The totality of all neighborhoods of the type U^* obtained by an arbitrary choice of a neighborhood U and a path l forms by definition a complete system Σ^* of neighborhoods of the space S. The space S is called a covering space for the space R, or more precisely the *universal covering space for R.*

We shall show that the complete system Σ^* of neighborhoods of the space S which was constructed in Definition 43 satisfies all the conditions of Theorem 3 and therefore S is really a topological space.

Let A and B be two distinct points of the space S. We shall show that there exists a neighborhood U^* of the point A which does not contain the point B. We distinguish two cases: a) Let $\varphi(A) \neq \varphi(B)$. Then we define the neighborhood U^* by means of a certain neighborhood U of the point $\varphi(A)$, which does not contain the point $\varphi(B)$, and by means of a path $l \in A$. It can readily be seen that with this choice of U, the set $\varphi(U^*)$ does not contain the point $\varphi(B)$ and therefore U^* does not contain B. b) Let now $\varphi(A) = \varphi(B) = a$. Since R is locally simply connected, there exists a neighborhood U of a such that every closed path beginning at a and going through U is homotopic to zero in the space R. We now define the neighborhood U^* by means of a neighborhood

$U \subset R$, and a path $l \varepsilon A$. Suppose that $B \varepsilon U^*$. This means that U contains a path x beginning at a such that $lx \varepsilon B$, but then the end of the path lx coincides with the point a, i.e. the path x is closed. Because of the construction of the neighborhood U the path x is homotopic to zero in R and therefore $lx \sim l$, i.e., $A = B$, which contradicts $A \neq B$.

Let now U^* and V^* be two neighborhoods of the point $A \varepsilon S$. We shall show that there exists a neighborhood W^* of the point A which is contained in the intersection $U^* \cap V^*$. Suppose that the neighborhoods U^* and V^* are defined by the neighborhoods U and V of R. We can use the path $l \varepsilon A$ as the path defining both the neighborhoods U^* and V^*, since $A \varepsilon U^*$ and $A \varepsilon V^*$. Since the end of the path l lies in the intersection of the neighborhoods U and V there exists a neighborhood W of the end of the path l such that $W \subset U \cap V$. We define the neighborhood W^* by means of the neighborhood W and the path l. Then it is easily seen that $W^* \subset U^* \cap V^*$.

Hence S is a topological space.

THEOREM 58. *The natural mapping φ of the covering space S on the space R* (see Definition 43) *is a continuous open mapping* (see Definition 15 and §18, C)). *Moreover, the mapping φ is a locally homeomorphic mapping i.e., for every point $A \varepsilon S$ there exists a neighborhood U^* such that the mapping φ is homeomorphic on the neighborhood U^** (see Definition 14).

PROOF. We first establish the continuity of the mapping φ. Let $A \varepsilon S$ and $\varphi(A) = a$. We denote by U an arbitrary neighborhood of the point a. We define the neighborhood U^* of the point A by means of the neighborhood U and the path $l \varepsilon A$. Obviously $\varphi(U^*) \subset U$. Hence the mapping φ is continuous.

We show next that φ is an open mapping. Let A be a point of the space S and U^* a neighborhood of A. Suppose U^* is defined by the neighborhood U and the path $l \varepsilon A$. Since the space R is by assumption locally connected, there exists a neighborhood V of the point $a = \varphi(A)$ such that for $x \varepsilon V$ there exists a path in U which begins at a and ends at x. It follows from this choice of the neighborhood V that $\varphi(U^*) \supset V$. Hence φ is an open mapping.

We shall show that the mapping φ is locally homeomorphic. Let $A \varepsilon S$, and $\varphi(A) = a$. Since the space R is locally simply connected there exists a neighborhood U of the point a such that every closed path beginning at a and contained in U is homotopic to zero in the space R. We now define a neighborhood U^* of the point A by means of the neighborhood U and a path $l \varepsilon A$. We shall show that the mapping φ is one-to-one on the set U^*. Suppose there exist two different points Y and Y' of the set U^* such that $\varphi(Y) = \varphi(Y')$. This means that U contains two paths x and x' beginning at a such that $lx \varepsilon Y$, $lx' \varepsilon Y'$ and such that the ends of these paths coincide. Then the path $x'x^{-1}$ is a closed path beginning at a and contained in U, and is therefore homotopic to zero in R; hence $lx \sim lx'$ (see E) and (1)). It follows from the last relation that $Y = Y'$. Hence we have arrived at a contradiction and the mapping φ is one-

to-one on U^*. Since the mapping φ is thus continuous, open, and one-to-one, it follows that it is homeomorphic on U^*. This proves Theorem 58.

In the process of proof of Theorem 58 we made use of the local connectedness and the local simple connectedness of the space R. The connectness of the space R is used when we suppose that φ is a mapping on the whole space R.

J) Let l be a curve in the space R with a fixed beginning p, which depends on one or several parameters, say $l = l(s)$. We denote by $F(s)$ that element of the covering space S (see Definition 43) which considered as a class of curves, contains the curve $l(s)$. If the curve $l(s)$ depends continuously on the parameter s, then the element $F(s)$ also depends continuously on s in the space S.

Let $f(s, t)$ be the function which defines the curve $l(s)$ for a fixed s. The point $f(s, 1)$ is the end of the curve $l(s)$ and depends continuously on the parameter s. Let σ be some value of the parameter s and let U^* be a neighborhood of the point $F(\sigma)$. We can suppose that U^* is defined by some neighborhood $U \subset R$ and by the curve $l(\sigma)$. Let ϵ be a sufficiently small positive number so that for $|s - \sigma| < \epsilon$ we have $f(s, 1) \varepsilon U$. We shall show then that for $|\sigma' - \sigma| < \epsilon$ we have $F(\sigma') \varepsilon U^*$. We introduce the curve $k(s)$, which depends continuously on the parameter s, and which is defined by the following function of t: $f(s + (\sigma' - s)t, 1)$. It can readily be seen that the beginning of the curve $k(s)$ coincides with the end of the curve $l(s)$, and therefore the product $l(s)k(s) = m(s)$ is defined. The curve $m(s)$ depends continuously on the parameter s and has fixed end points: therefore $m(\sigma) \sim m(\sigma')$. Furthermore $k(\sigma')$ is a null path and therefore $m(\sigma') \sim l(\sigma')$. Hence $m(\sigma) \sim l(\sigma')$. But $k(\sigma)$ is a path contained in U. Therefore $F(\sigma') \varepsilon U^*$. Hence the element $F(s)$ depends continuously on the parameter s. The case involving several parameters can be similarly disposed of.

K) The covering space S of the space R (see Definition 43) is connected, locally connected, and locally simply connected.

It follows from Theorem 58 that the spaces R and S are locally homeomorphic; therefore all the local properties of the space R are automatically true for the space S.

We shall show that S is connected. Let $A \varepsilon S$ and let P be that point of the space S which considered as a class of paths contains a null path. To prove that S is connected, it is sufficient to show that the point A can be connected by a curve to the point P, since A is an arbitrary point while P is fixed. Let $l \varepsilon A$, and let $f(t)$ be the function which defines the path l. Let us consider the family of paths which depend on the parameter s, and which are defined by the function $f(st)$. For a fixed s, $0 \leqq s \leqq 1$, this function defines a path $l(s)$ in the space R, with $l(0) \varepsilon P$, and $l(1) = l \varepsilon A$. We denote by $A(s)$ the class of paths which contains the path $l(s)$. $A(s)$ is a point of the space S which depends continuously on the parameter s (see J)). Hence $A(s)$ defines in the space S a path which connects the point P to the point A.

The following theorem states the fundamental property of the universal covering space.

THEOREM 59. *The universal covering space S of a topological space R* (see Definition 43) *is always simply connected* (see G)).

PROOF. Let us denote by P that element of the space S which considered as a class of paths contains a null path. We shall show that a closed curve L in the space S which begins at the point P is homotopic to zero in S.

Let $F(t)$ be the function which defines the curve L, and let $f(t) = \varphi(F(t))$, where φ is the natural mapping of the space S on the space R (see Definition 43). The function $f(st)$ defines for a fixed s, $0 \leqq s \leqq 1$, a certain path $l(s)$ which begins at p (see Definition 43) and depends continuously on s. We denote by $F'(s)$ that element of the space S, which considered as a class of paths contains the path $l(s)$. We shall then show that

$$F'(s) = F(s). \tag{6}$$

It can readily be seen first of all that

$$\varphi(F'(s)) = \varphi(F(s)).$$

For $s = 0$, the equation (6) is obvious. If now equation (6) is true for all values of $s < \sigma$, then it is true for $s = \sigma$, since $F(s)$ and $F'(s)$ are continuous functions of the parameter s (see J)). Furthermore, if equation (6) holds for $s = \sigma$, then for a sufficiently small h, it also holds for $s = \sigma + h$. In fact let U^* be that neighborhood of the point $F'(\sigma) = F(\sigma)$ for which the mapping φ is one-to-one (see Theorem 58). Then for a sufficiently small h we have $F'(\sigma + h) \varepsilon U^*$, $F(\sigma + k) \varepsilon U^*$. But in view of the fact that the mapping φ is one-to-one, and because of equation (7), $F'(\sigma + h) = F(\sigma + h)$. Hence equation (6) is true for all values of s, $0 \leqq s \leqq 1$.

Since the curve L is closed, $F(1) = P$ and therefore (see (6)) $l(1)$ is a curve which is homotopic to zero. Let $l(s, t)$ be the function which exhibits the homotopy to zero of the curve $l(1)$ (see B)). The function $\varphi(s, \tau t)$ for s and τ fixed defines a curve $l(s, \tau)$ which depends continuously on the parameters s and τ. We denote by $\Phi(s, \tau)$ that element of the space S which considered as a class of paths contains the curve $l(s, \tau)$. The point $\Phi(s, \tau)$ depends continuously on the parameters s and τ (see J)). It is not hard to see that the function $\Phi(s, t)$ realizes the homotopy to zero of the curve L. This proves the theorem.

THEOREM 60. *Let R and S be two connected topological spaces* (see F)). *We denote by T their topological product* (see Definition 21). *Then the space T is connected and its fundamental group is isomorphic with the direct product of the fundamental groups of the spaces R and S* (see Definition 10′). *Hence, in particular, the topological product of two simply connected topological spaces* (see G)) *is simply connected.*

PROOF. Let us select a single fixed point from each of the spaces R and S: $p \varepsilon R$, $q \varepsilon S$. Then $(p, q) \varepsilon T$ is a definite point of T. Let k be a path in the space R which begins at p and is defined by the function $f(t)$, and let l be a

path in the space S which begins at q and is defined by the function $g(t)$. Then the function $(f(t), g(t))$ defines a certain path in the space T, which we shall denote by (k, l). Then (k, l) begins at the point (p, q) and ends at the point $(f(1), g(1))$. Since the spaces R and S are connected the end points of the paths k and l can be selected arbitrarily, and hence the endpoint of the path (k, l) can also be selected arbitrarily so that the point (p, q) can be joined by a path with an arbitrary point of the space T. Hence T is connected.

Obviously every path m of the space T which begins at (p, q) can be represented by the pair (k, l). It is not hard to verify that if $k' \sim k$ and $l' \sim l$, then $(k', l') \sim (k, l)$. The converse is also true i.e., if $(k', l') \sim (k, l)$, then $k' \sim k$, and $l' \sim l$. If k and l are closed, then the path (k, l) is also closed, and conversely. Finally if the paths k, l, k', l' are all closed, then the product $(k, l)(k', l')$ is equal to (kk', ll').

It follows from what has just been said that every element of the fundamental group of the space T is uniquely represented in the form of a pair of elements of the fundamental groups of the spaces R and S in such a way that all the conditions of Theorem 10′ hold. Hence Theorem 60 is proved.

47. The Universal Covering Group

In this section we develop the results of Schreier. The main idea consists in constructing a covering space for every topological group, and then showing that this covering space itself forms a topological group in a natural way. The group thus obtained is called the universal covering group of the original group.

Because the constructions of this section depend entirely on the results of the preceding section we must limit ourselves by the following conditions:

A) All the topological groups considered in this section are connected, locally connected, and locally simply connected (see §46, F), I), and H)).

It is not hard to verify that Lie groups (see Definition 38) which are connected in the ordinary sense (see §11, A)) satisfy the above conditions. Therefore the results of this chapter are applicable to connected Lie groups.

Theorem 61. *There exists for every topological group G a simply connected topological group G^** (see §46, G)) *which is locally isomorphic with it, and is such that the group G is isomorphic with the factor group G^*/N, where N is a discrete normal subgroup of the group G^*, and the fundamental group of the space G* (see Definition 42) *is isomorphic with the group N.* (We suppose here that the group G satisfies condition A); then the group G^* also satisfies the condition A).)

Proof. We construct the universal covering space G^* for the topological space G, by taking the identity e of the group G for the fundamental point p (see Definition 43). In this way G^* is a topological space satisfying conditions A) (see §46, K)), and there exists a natural mapping φ of the space G^* on the space G, which is a continuous open mapping (see Theorem 58).

We now introduce into G^* the group operation of multiplication. Let A and

B be any two elements of the set G^*. We denote by k a path in the class A, and by l a path in the class B. Both these paths begin at the identity e of the group G, while we designate the ends of these paths by a and b. Then

$$\varphi(A) = a, \qquad \varphi(B) = b.$$

Let $g(t)$ be the function defining the path l (see §46, A)). The function $ag(t)$ defines a new path, which we denote by al (here the product $ag(t)$ is taken in the sense of the group operation in G). It can be seen readily that

(1) $$\text{if} \quad l \sim l' \quad \text{then} \quad al \sim al'.$$

The paths k and al can be multiplied since the end of the first coincides with the beginning of the second. We denote by C the class of paths which contains the path $m = k(al)$. The element C is defined uniquely by the classes A and B, i.e., it does not depend on the choice of the paths k and l of the classes A and B (see (1) and §46, (1)). The product AB is defined by letting $AB = C$. We note that the end of the paths of C is ab and hence

(2) $$\varphi(AB) = \varphi(A)\varphi(B).$$

We shall show that the operation of multiplication defined on G^* satisfies all the group axioms. To prove associativity we make use of the obvious fact that if k' and l' are two paths in G which can be multiplied together, and if $a' \in G$, then

(3) $$a'(k'l') = (a'k')(a'l').$$

Now let A, B, and C be three elements of G^*. We denote by k, l, and m three paths selected from A, B, and C, and denote their ends by a, b, and c. By the law of multiplication $A(BC)$ is defined as the class which contains the path

$$k(a(l(bm))) = n,$$

while the product $(AB)C$ is defined as the class containing

$$(k(al))(abm) = n'.$$

From (3) we have

$$n = k((al)(abm)).$$

Hence $n \sim n'$ (see §46, D)), and multiplication is associative in G^*. The identity of the group G^* is the class E which contains all the paths homotopic to zero. To find the element A^{-1} inverse to the element A, we denote by l some path of the class A and by a the end of this path. The class containing the path $a^{-1}l^{-1}$ we denote by B It is not hard to see that $AB = E$. For by the law of multiplication AB is defined as the class containing the path $l(aa^{-1}l^{-1})$. But this path is homotopic to zero (see §46, E)). Hence $A^{-1} = B$ and the inverse element always exists in G^*. Hence all the group axioms are satisfied in G^*.

We shall show that the group operations taking place in G^* are continuous in the topological space G^*, and hence G^* is a topological group.

Let A and B be two elements of G^* and let $C = AB$. We denote by W^* a neighborhood of the element C, and select from A and B the paths k and l, whose ends we denote by a and b. Then $m = k(al) \varepsilon C$, and we can assume that the neighborhood W^* is defined by a certain neighborhood $W \subset G$, and by the path m (see Definition 43). We have $ab \varepsilon W$, and therefore there exist neighborhoods U and V of the elements a and b such that

$$(4) \qquad UV \subset W.$$

The neighborhood U^* of the element A is defined by the neighborhood U and the path k. In the same way the neighborhood V^* of the element B is defined by the neighborhood V and the path l. An arbitrary element A' of the neighborhood U^* is defined as the class which contains the path kx, where x is an arbitrary path beginning at a and contained in U. Let $f(t)$ be the function which defines the path x. For a fixed s, $0 \leqq s \leqq 1$, the function $f(st)$ defines the path $x(s)$. Let $k(s) = kx(s)$, and let $k(s)$ be a continuous function of s, with $k(0) = k$, $k(1) = kx$. We make an analogous construction for the neighborhood V and denote the variable path there obtained by $l(s)$, where $l(0) = l$ and the path $l(1)$ defines an arbitrary preassigned element B' of the neighborhood V^*. We denote the end of the path $k(s)$ by $a(s)$, and let $m(s) = k(s)(a(s)l(s))$. We have $m(0) \varepsilon AB$, $m(1) \varepsilon A'B'$. We have to show that $A'B' \varepsilon W^*$, and to do this it is sufficient to show that the path $m(1)$ is homotopic to the path $m(0)z$, where z is a path going through W. We denote by $c(s)$ the end of the variable $m(s)$. The point $c(s)$ describes for $0 \leqq s \leqq 1$ a certain path which is entirely contained in W (see (4)) and which we denote by z. Obviously $m(1) \sim m(0)z$. Hence $A'B' \varepsilon W^*$, and $U^*V^* \subset W^*$, and this means that the operation of multiplication is continuous. In the same way we can show that the operation of taking an inverse of an element is also continuous. Hence G^* is a topological group.

As we have already noted, φ is an open continuous mapping of the topological space G^* on the topological space G. It follows from (2) that this mapping is an open homomorphic mapping of the topological group G^* on the topological group G. We denote by N the kernel of the homomorphism φ. Since φ is a locally homeomorphic mapping (see Theorem 58), there exists a neighborhood U^* of the identity of the group G^* which admits a one-to-one mapping, and this means that N is a discrete normal subgroup of the group G^*. By Theorem 12 the group G is isomorphic with the factor group G^*/N.

We consider in greater detail the set N. If $A \varepsilon N$, then $\varphi(A) = e$, and hence all the paths of the class A are closed. Conversely if all the paths of the class A are closed, then $\varphi(A) = e$ and $A \varepsilon N$. Therefore N is composed of all classes of closed paths, i.e., N, considered as a set, coincides with the fundamental group of the topological space G (see Definition 42). It is not hard to see, furthermore, that if A and B are two closed paths which begin at e, then the

law of multiplication which we have established for the elements A and B of the group G^* simply coincides with the multiplication law which holds for the elements A and B of the fundamental group. Therefore N coincides with the fundamental group of the space G. This proves Theorem 61.

The following rather interesting result is a direct consequence of Theorem 61.

THEOREM 62. *If G is a topological group satisfying conditions* A), *then the fundamental group of the topological space G* (see Definition 42) *is commutative.*

PROOF. By Theorem 61 the fundamental group of the topological space G is isomorphic with the discrete normal subgroup N of the connected topological group G^*. Since G^* is connected, it follows from Theorem 16 that the normal subgroup N of this group is commutative. Hence the fundamental group of the space G is commutative.

In view of some further applications we formulate Theorem 63 which follows in a more general form than is necessary for the purposes of the present chapter. Instead of limiting ourselves to local isomorphism we introduce here the concept of local homomorphism.

B) Let G' and G be two topological groups and let U be a neighborhood of the identity in the group G. Suppose that there exists a continuous mapping f of the set U in the space G' such that for $x \varepsilon U$, $y \varepsilon U$, and $xy \varepsilon U$, we have $f(xy) = f(x)f(y)$. We shall then say that f is a *local homomorphism* of the group G in the group G'. If f is an open mapping of U on a certain neighborhood of the identity of the group G', then we shall say that f is a local homomorphism of the group G *on* the group G'. In case f is a homeomorphic mapping on some neighborhood of the identity of the group G', we get the old concept of local isomorphism.

The following theorem plays a rather important part.

THEOREM 63. *Let G' and G be two connected topological groups, and let G be locally connected and also simply connected* (see §46, G), and J)). *We do not require that G' satisfy the conditions of* A). *Let f be some local homomorphism of the group G in the group G'* (see B)). *Then it is possible to extend uniquely the local homomorphism f into a homomorphism φ of the entire group G in the entire group G'. The extension of the homomorphism f is understood in the sense that f and φ coincide on some neighborhood $W \subset U$ of the identity of the group G, where U is the neighborhood in which the local homomorphism f is defined. If f is a local homomorphism of the group G on the group G', then φ is a homomorphism of the group G on the group G'. If f is a local iomorphism, then the homomorphism φ is open. If the group G' is simply connected and satisfies condition* A) *and if f is a local isomorphism, then the homomorphism φ is an isomorphism.*

PROOF. We shall show first of all that if φ is a homomorphic mapping of the abstract group G in the abstract group G', where φ is an extension of the local homomorphism f, then φ is a homomorphic mapping of the topological group G in the topological group G'. In fact in the neighborhood W the functions f

and φ coincide, and since the function f is continuous, the function φ is everywhere continuous (see §19, B)).

If f is a locally homomorphic mapping of the group G on the group G', then the extension φ is a homomorphism of the group G on the group G'. In fact in this case $f(W)$ contains a certain neighborhood of the identity, and since a connected group G' can be generated by any neighborhood of its identity (see Theorem 15), it follows that every element $x' \varepsilon G'$ can be represented in the form $x' = \varphi(x)$.

If f is a local isomorphism, then its extension φ is an open homomorphism. In fact, in this case the mapping f is homeomorphic and hence the mapping φ is open in the neighborhood of the identity, and therefore it is always open (see §19, B)).

We shall show that the extension of the homomorphism f to the homomorphism φ can be accomplished in only one way. Suppose that there exist two extensions φ and φ'. Let x be an arbitrary element of G and let W be that neighborhood of the identity in the group G on which φ and φ' coincide with f. Since G is connected, it follows from Theorem 15 that every element x can be represented in the form $x = a_1 \cdots a_n$, where $a_i \varepsilon W$, $i = 1, \cdots, n$. Hence we have

$$\varphi(x) = f(a_1) \cdots f(a_n)$$
$$\varphi'(x) = f(a_1) \cdots f(a_n)$$

and

$$\varphi(x) = \varphi'(x).$$

We now proceed to construct the homomorphism φ. Let l be a curve in G which begins at the identity e of the group G. We denote the function which defines this curve by $g(t)$. We construct for the curve l a curve l' which uniquely corresponds to it in the space G', and which is such that its defining function $g'(t)$ satisfies the following conditions: a) $g'(0) = e'$, where e' is the identity of the group G', b) there exists a sufficiently small positive number ϵ such that for $|t_1 - t_2| \leqq \epsilon$, $(g(t_1))^{-1}g(t_2) \varepsilon U$ and $(g'(t_1))^{-1}g'(t_2) = f((g(t_1)^{-1}g(t_2))$.

We shall show first of all that if the curve l' exists, then it is defined uniquely by conditions a) and b). The beginning of the curve l' is defined by condition a). Furthermore, if the curve l' is defined uniquely for all values of $t < \tau$, then it is defined for $t = \tau$ because of the continuity of the functions $g(t)$ and $g'(t)$. Finally if the function $g'(t)$ is defined for $t = \tau$, then it is defined for all t such that $t - \tau < \epsilon$. In fact by b), $g'(t) = g'(\tau)f((g(\tau))^{-1}g(t))$. Therefore the curve l' is defined uniquely for all values of t.

We shall show now that the curve l' exists. Let V be a neighborhood of the identity of the group G such that $V^{-1}V \subset U$. There exists a sufficiently large number n such that for $|t_1 - t_2| \leqq 1/n$ we have $(g(t_1))^{-1}g(t_2) \varepsilon V$. Let $\epsilon = 1/n$ and suppose that the function $g'(t)$ is already defined for all values of $t \leqq m\epsilon$, and that conditions a) and b) hold for these values of t. We shall show that

this function can be extended further. Let h be a positive number not exceeding ϵ. We then defined $g'(m\epsilon + h)$ by setting

$$g'(m\epsilon + h) = g'(m\epsilon)f((g(m\epsilon))^{-1}g(m\epsilon + h)). \tag{5}$$

We shall show that condition b) now holds for the extended function $g'(t)$. Let h' be a number not exceeding ϵ in absolute value. We then have

$$g'(m\epsilon + h') = g'(m\epsilon)f((g(m\epsilon))^{-1}g(m\epsilon + h')). \tag{6}$$

If h' is positive, relation (6) follows from (5), and if h' is negative, (6) follows from the assumption of the induction. Hence

$$(g'(m\epsilon + h))^{-1}g'(m\epsilon + h') = f((g(m\epsilon + h))^{-1}g(m\epsilon + h'))$$

and condition b) is also satisfied. To start the induction at $m = 0$ it is sufficient to let $g'(0) = e'$. Then condition a) will always hold. Hence the induction is completed and the curve l' constructed.

Let now t_1 and t_2 be two numbers such that $0 \leqq t_1 < t_2 \leqq 1$, where $|t_2 - t_1| \leqq \epsilon$. If the curve l is subjected to a continuous deformation which only changes its points in the interval $t_1 < t < t_2$, then, obviously, the corresponding curve l' is also changed only on that interval, since the above construction of the curve l' for values of $t \leqq t_1$ depends only on the curve l in the interval $t \leqq t_1$. Furthermore, for $t = t_2$ the function $g'(t)$ is defined by condition b) from the value of the function $g'(t_1)$, while the further development of the curve l' depends only on the value of $g'(t_2)$. We shall call such a deformation of the curve l a *small* deformation. We have just shown that under a small deformation of the curve l the corresponding curve l' is also subjected to a small deformation, and in particular does not change its end point.

It is not hard to show that any deformation of the curve l which leaves its ends unaltered can be achieved by means of a series of small deformations. Therefore if we subject the curve l to any continuous deformation which preserves its ends, then the corresponding curve l' also undergoes a continuous deformation which does not change its ends.

Let x be an arbitrary point of G and l a curve which connects the identity e to the point x. Let l' be the curve which corresponds to the curve l, and let x' be the end of the curve l'. We shall show that the point x' is defined by the point x and does not depend on the choice of l. In fact, let k be another curve which connects e and x. Since G is simply connected, the curves k and l are homotopic, and therefore they can be transformed into each other by a continuous deformation. From what we have already shown the corresponding curve in G' will not change its ends during this process, and therefore the point x' is defined by the curve k as well as by the curve l. Hence we can suppose that $x' = \varphi(x)$.

We shall now show that there exists a neighborhood $W \subset U$ of the identity of the group G on which $\varphi = f$. Let V be a neighborhood of the identity of the group G such that $V^{-1}V \subset U$. We define $W \subset V$ as a neighborhood of the

identity of the group G which is such that there exists a curve $l \subset V$ which connects every point x of V with e (such a neighborhood exists since the group G is locally connected). Let $g(t)$ be the parametric representation of the curve $l \subset V$. It can be seen readily that the curve l' which is defined in parametric form by the condition $g'(t) = f(g(t))$ satisfies condition b) of our construction. In fact since $g(t) \subset V$, it follows that $(g(t))^{-1} \subset V^{-1} \subset U$, and for any t_1 and t_2, $(g(t_1))^{-1}g(t_2) \subset V^{-1}V \subset U$, and hence $f((g(t_1))^{-1}g(t_2)) = f((g(t_1))^{-1})f(g(t_2)) = (f(g(t_1)))^{-1}f(g(t_2)) = (g'(t_1))^{-1}g'(t_2)$. Hence the end of the curve l' is $f(x)$, where x is the end of the curve l, i.e., $\varphi(x) = f(x)$ for $x \varepsilon W$.

We shall show that the mapping φ is a homomorphic mapping of the abstract group G in the abstract group G'.

Let a and b be two arbitrary points of G. We denote by k and l the curves which connect e to a and b, and by k' and l' the curves which correspond to k and l, and which have their ends at a' and b'. Obviously, the curve $k(al) = m$ connects the identity e to the point ab, while the corresponding curve $k'(a'l') = m'$ goes from e' to $a'b'$. It is not hard to verify that the curve m' corresponds to the curve m. Hence, because of the way in which the mapping φ was constructed, we have $\varphi(ab) = a'b'$, and this means that $\varphi(ab) = \varphi(a)\varphi(b)$, i.e., the mapping φ is homomorphic.

It remains to consider only the case in which G' is a simply connected group satisfying conditions A), and f a local isomorphism. If the neighborhood U is chosen sufficiently small, then the mapping f^{-1} is a local isomorphism of the group G' in G. Since G' is supposed to be simply connected, and since it satisfies conditions A), it follows from the above that the local isomorphism f^{-1} can be extended into an open homomorphism ψ of the group G' on the group G. The mapping $\psi(\varphi(x)) = \chi(x)$ is a homomorphic open mapping of the group G into itself. In a sufficiently small neighborhood of the identity of the group G, the mapping $\chi(x)$ coincides with the mapping $f^{-1}(f(x)) = x$. Hence χ is an extension of an identical local automorphism of the group G. Because of the uniqueness of the continuation of a mapping, the mapping χ is the identical mapping of the group G into itself, and this means tha tthe mappings φ and ψ are inverses of each other. Hence φ is a unique inverse mapping and therefore φ is an isomorphic mapping. This completes the proof of Theorem 63.

THEOREM 64. *Let G' be a simply connected topological group satisfying conditions* A), *and let N' be a discrete normal subgroup of the group G'. Then the fundamental group of the topological space $G'/N' = G$ is isomorphic with the group N'.*

PROOF. We denote by ψ the natural homomorphic mapping of the topological group G' on the topological group G. Since N' is a discrete normal subgroup, the mapping ψ represents a local isomorphism of the group G in the group G' (see §23, C)) in a sufficiently small neighborhood of the identity of the group G'. Now let G^* be that simply connected group which was constructed for the group G in Theorem 61, and let N be a discrete normal sub-

group of G^* such that G is isomorphic with G^*/N. We denote the natural homomorphic mapping of the group G^* on the group G by φ. The mapping φ represents a local isomorphism of the group G in G^* in a small neighborhood of the identity; therefore the mapping $\varphi^{-1}(\psi(x)) = f(x)$ is defined and represents a local isomorphism of the group G' in G^*. Since the groups G' and G^* are simply connected, the local isomorphism f can be extended into an isomorphism χ of the group G' on the group G^* (see Theorem 63). Furthermore, the mapping $\psi(x)$ coincides locally with $\varphi(\chi(x))$ and hence $\psi(x) = \varphi(\chi(x))$ because of the uniqueness of the extension of a local isomorphism. Hence the normal subgroup N' goes over into the normal subgroup N under the isomorphism χ, i.e., N and N' are isomorphic groups. By Theorem 61 the fundamental group of the space G is isomorphic with the group N, and hence it is also isomorphic with the group N'. This proves Theorem 64.

The above theorems enable us to formulate the following definition.

Definition 44. Let Δ be the aggregate of all topological groups satisfying conditions A) and locally isomorphic with one such group. By Theorem 61, the set Δ contains at least one simply connected group, which we denote by G^*. It follows from Theorem 63 that up to an isomorphism the set Δ contains *only* one simply connected group. Hence the group G^* is defined uniquely by the set Δ. G^* is called the *universal covering group* for all the groups of the set Δ.

It follows from Theorem 61 that every group G of the set Δ can be written in the form G^*/N, where N is some discrete normal subgroup of the group G^*, By Theorem 16, N is a central normal subgroup of the group G^*, while Theorem 64 shows that N is isomorphic with the fundamental group of the space G.

Hence in order to obtain all the groups of the set Δ, it is sufficient to know all central discrete subgroups of the group G^*. We must therefore study in detail all the discrete subgroups of the center Z of the group G. This does not present any great difficulty because the center is commutative.

Example 60. Let G^* be the r-dimensional vector group, and N the subgroup of G^* composed of all vectors whose coordinates are integers. The factor group $G^*/N = G$ is a toroidal r-dimensional group. It is not hard to see that the group G^* is simply connected and therefore is the universal covering group for the group G. The subgroup N, when considered as an abstract group, is a commutative group having r linearly independent generators. Such is also the fundamental group of the r-dimensional torus G.

In the next chapter we shall give more examples of topological groups, and also more complicated and more interesting examples of universal covering groups.

Example 61. We point out here one interesting generalization of Theorem 64. Let G be a simply connected group satisfying conditions A), and let H be a discrete subgroup of the group G (not necessarily a normal subgroup). Then the fundamental group of the space $G/H = R$ (see Definition 24) is isomorphic with the group H.

The proof of this proposition is as follows. We denote by φ the natural

mapping of the space G on the space R and let $\varphi(e) = p$, where e is the identity of the group G. Let l be a curve going from e to some point $h \varepsilon H$. The image $l' = \varphi(l)$ of the curve l in the space R is a closed curve. It can be shown, conversely, that every closed curve l' beginning in p can be obtained as the image of some curve l beginning at e and ending at H. It can be shown further that the curve l' is homotopic to zero if and only if the curve l is closed. In this way a one-to-one correspondence is established between the elements of the fundamental group of the space R and the elements of the group H. The isomorphism can readily be proved.

In the next chapter we give an example of a simply connected group G satisfying conditions A), which has a non-commutative discrete subgroup H (see Example 71). Hence the fundamental group of the topological space is in general non-commutative. This explains the particular interest of Theorem 62.

CHAPTER IX

THE STRUCTURE OF LIE GROUPS

The concept of Lie groups was defined in Chapter VI, where we established the simplest properties of Lie groups. We shall study Lie groups in greater detail here, making use of the results of Chapter VI. We shall associate with Lie groups more elementary algebraic entities, namely infinitesimal groups, and show that the local study of Lie groups can be reduced entirely to the study of infinitesimal groups. This is the main object of the present chapter. We shall also consider some related concepts, and indicate further developments of the theory. We shall not take up the deeper results of Killing, Cartan (see [5]), and Weyl (see [35]). These results depend on the properties of infinitesimal groups and represent a far reaching theory. We shall state some of them without proof. The most important result of the theory is a complete classification of simple Lie groups. This classification, however, necessitates such cumbersome and complicated considerations that it is impossible to consider it here. The reader will find a more detailed exposition of the theory of Lie groups in the forthcoming book of N.G. Chebotareff, on "The Theory of Lie Groups" (in Russian).

We have shown in Chapter VI that in studying Lie groups we can confine ourselves to triply differentiable functions of several variables. We can therefore avail ourselves here of the theory of differential calculus and differential equations. This will form the main method of investigation in the present chapter. Because of the extensive calculations which we meet, we shall make use here, as in Chapter VI of tensor notation.

48. Structural Constants. Infinitesimal Groups

We shall introduce here the structural constants of Lie groups. They form a tensor, i.e., they transform as components of a tensor under a transformation of coordinates in a Lie group. An infinitesimal group is an invariant with respect to coordinate transformations whose study is equivalent to that of the totality of structural constants. We shall establish here the fundamental relations between structural constants and the corresponding relations in the infinitesimal group.

The main method of the present section consists in expanding the functions under consideration in Taylor series up to terms of the second and sometimes third order. The study of the coefficients thus obtained introduces the structural constants as well as some of the relations between them. This could have been done by means of derivatives, but Taylor series seem more useful in this connection.

A) The remainders of the series will not be written out in detail but merely denoted by ϵ with different subscripts, but the order of magnitude of each ϵ

will be made clear. If ϵ depends on the arguments $x_1, \cdots, x_n$ we shall say that ϵ is of the *order of magnitude* $q + 1$ with respect to these arguments if ϵ/ρ^q, where $\rho = \sqrt{(x_1^2 + \cdots + x_n^2)}$, tends to zero with ρ.

B) In the future we shall denote the coordinates of a point or vector by the same letters used for that point or vector, but with superscripts. This will save us the necessity of introducing the notation each time.

Definition 45. Let G be an r-dimensional local Lie group and D a differentiable system of coordinates in it (see Definition 38). If x and y are two elements of the group G which are sufficiently close to the identity, then the product $f = xy = f(x, y)$ is also close to e and the law of multiplication can be written in coordinate form by means of the system D. We then have

$$(1) \qquad f^i = f^i(x, y) = f^i(x^1, \cdots, x^r; y^1, \cdots, y^r).$$

Since the coordinates of the identity are zero, we have:

$$(2) \qquad f^i(x, e) = f^i(x^1, \cdots, x^r; 0, \cdots, 0) = x^i$$

$$(3) \qquad f^i(e, y) = f^i(0, \cdots, 0; y^1, \cdots, y^r) = y^i.$$

Since the functions f^i have by assumption three continuous derivatives they can be expanded in a Taylor series up to terms of the third order. Because of (2) and (3) these expansions have a special form, which is not hard to find. In fact we have

$$(4) \qquad f^i = x^i + y^i + a^i_{jk}x^j y^k + g^i_{jkl}x^j x^k y^l + h^i_{jkl}x^j y^k y^l + \epsilon^i_1,$$

where ϵ^i_1 is a quantity of the fourth order of magnitude with respect to the coordinates of the points x and y. The numbers

$$(5) \qquad c^i_{jk} = a^i_{jk} - a^i_{kj}$$

are called the *structural constants* of the group G in the coordinates D.

The structural constants satisfy the relation

$$(6) \qquad c^i_{jk} = -c^i_{kj}.$$

Relations (4) show that a Lie group is in the first approximation commutative and isomorphic with an r-dimensional vector group. The second approximation, however, already deviates from commutativity. It is not hard to show that even a commutative group may in some coordinates have an expansion (4) with non-zero terms of the second order. But in case G is commutative we have obviously $a^i_{jk} = a^i_{kj}$, and therefore the structural constants are zero for a commutative group. This is the first indication that the structural constants play an important part in the theory of Lie groups. Later we shall show that the structural constants define completely the local structure of Lie groups, which explains the terminology used.

We shall give here another definition of structural constants, which throws further light on their nature.

C) Let x and y be two elements of the group G. We consider the commutator q (see §4, C)) of the elements x and y

$$q = xyx^{-1}y^{-1} = q(x, y). \tag{7}$$

In coordinate form equation (7) may be written

$$q^i = c^i_{jk}x^j y^k + \epsilon^i_2 \tag{8}$$

(see (5)), where ϵ^i_2 is a quantity of the third order of magnitude with respect to the coordinates of the points x and y. Relation (8) may be used as a new definition of structural constants. It follows from (4), (5) and (8) that

$$q^i(x, y) = f^i(x, y) - f^i(y, x) + \epsilon^i_3, \tag{9}$$

where ϵ^i_3 is also of the third order of magnitude.

In order to prove relation (8) we calculate first of all the element z' inverse to z, $zz' = e$, in coordinate form. Using (4) we have

$$z'^i = -z^i + a^i_{jk}z^j z^k + \epsilon^i_4. \tag{10}$$

If now $z^* = xy$, and $z = yx$, then by (4), (5), (7), and (10) we have $q = z^*z'$ and

$$\begin{aligned} q^i = {} & (x^i + y^i + a^i_{jk}x^j y^k) + (-x^i - y^i - a^i_{kj}x^j y^k + a^i_{jk}(x^j + y^j)(x^k + y^k)) \\ & - a^i_{jk}(x^j + y^j)(x^k + y^k) + \epsilon^i_2 = c^i_{jk}x^j y^k + \epsilon^i_2. \end{aligned}$$

Hence (8) is proved.

THEOREM 65. *The structural constants of a Lie group G satisfy the following relations:*

$$c^p_{ij} = -c^p_{ji} \tag{11}$$

and

$$c^p_{is}c^s_{jk} + c^p_{js}c^s_{ki} + c^p_{ks}c^s_{ij} = 0. \tag{12}$$

Relation (12) is closely connected with the associativity of multiplication in the group G.

PROOF. Relation (11) has already been proved (see (6)). To prove (12) it is sufficient to express the associativity of multiplication in coordinate form. Let

$$u = yz, \qquad v = xy, \qquad w = xu, \qquad w' = vz.$$

We then write the equality $w = w'$ in coordinate form. Using (4) and carrying out our calculations up to terms of the third order we get

$$\begin{aligned} w^p = {} & x^p + (y^p + z^p + a^p_{jk}y^j z^k + g^p_{ijk}y^i y^j z^k + h^p_{ijk}y^i z^j z^k) \\ & + a^p_{is}x^i(y^s + z^s + a^s_{jk}y^j z^k) + g^p_{ijk}x^i x^j(y^k + z^k) \\ & + h^p_{ijk}x^i(y^j + z^j)(y^k + z^k) + \epsilon^p_5, \end{aligned}$$

$$
\begin{aligned}
w'^p = {} & (x^p + y^p + a^p_{ij}x^iy^j + g^p_{ijk}x^ix^jy^k + h^p_{ijk}x^iy^jy^k) + z^p \\
& + a^p_{sk}(x^s + y^s + a^s_{ij}x^iy^j)z^k + g^p_{ijk}(x^i + y^i)(x^j + y^j)z^k \\
& + h^p_{ijk}(x^i + y^i)z^jz^k + \epsilon^p_6,
\end{aligned}
$$

where ϵ^p_5 and ϵ^p_6 are of the fourth order of magnitude.

The comparison of the terms of the first order in the expressions for w^p and w'^p gives

$$x^p + (y^p + z^p) = (x^p + y^p) + z^p$$

while the comparison of the terms of the second order gives

$$a^p_{jk}y^jz^k + a^p_{is}x^iy^s + a^p_{is}x^iz^s = a^p_{ij}x^iy^j + a^p_{sk}x^sz^k + a^p_{sk}y^sz^k$$

so that the equality for the terms of the first and second order holds identically.

We now pass to the comparison of the terms of the third order. In doing so we shall limit ourselves to those terms which depend on the coordinates of all three points x, y and z, since the equality should hold for them separately. As a matter of fact all the other terms of the third order are identically equal, but that does not concern us. We then have

$$a^p_{is}x^ia^s_{jk}y^jz^k + h^p_{ijk}x^i(y^jz^k + y^kz^j) = a^p_{sk}a^s_{ij}x^iy^jz^k + g^p_{ijk}(x^iy^j + x^jy^i)z^k.$$

Equating coefficients in the last relation we get

$$a^p_{is}a^s_{jk} - a^p_{sk}a^s_{ij} = -h^p_{ijk} - h^p_{ikj} + g^p_{ijk} + g^p_{jik}. \tag{13}$$

We now eliminate from this last relation the members on the right side. To do so we permute the indices i, j, k in all possible ways. The six relations thus obtained are called odd or even depending on whether the corresponding permutation of the indices is odd or even. We now add these six relations by taking the even ones with the plus sign and the odd ones with the minus sign. The relation so obtained as the sum, which we denote by (a), has zero in the right side and twelve terms in the left side. If we now replace the structural constants in relation (12) by their expressions from (5), we get a new relation (b), which also contains twelve terms in the left side, and zero in the right side. It is not hard to guess from the general character of the terms that relations (a) and (b) coincide. Therefore, relation (12) is a consequence of relations (13) and (5). This proves Theorem 65.

We now proceed to the construction of an infinitesimal group.

Definition 46. Let R be the r-dimensional vector space in which the following operation of composition of vectors is defined: to every pair of vectors a and b corresponds a vector $c = [a, b]$, which is called the *commutator* of the vectors a and b. This operation satisfies the following conditions:

$$[\alpha a + \alpha' a', b] = \alpha[a, b] + \alpha'[a', b]. \tag{14}$$

where α and α' are real numbers. Furthermore,

$$[a, b] + [b, a] = 0, \quad \text{and} \tag{15}$$

$$[a, [b, c]] + [b, [c, a]] + [c, [a, b]] = 0. \tag{16}$$

We shall call the vector space R, together with the operation of commutation established in it, an *infinitesimal group.*

Since the operation of commutation is linear (see (14), (15)), it can be written in coordinate form as follows

$$c^i = [a, b]^i = c_{jk}^{\cdot\cdot i} a^j b^k. \tag{17}$$

The numbers $c_{jk}^{\cdot\cdot i}$ are called the *structural constants* of the infinitesimal group R in the given system of coordinates. From relations (15) and (16) we obtain the following relations for the structural constants of the infinitesimal group R:

$$c_{jk}^{\cdot\cdot i} = - c_{kj}^{\cdot\cdot i}, \tag{18}$$

$$c_{is}^{\cdot\cdot p} c_{jk}^{\cdot\cdot s} + c_{js}^{\cdot\cdot p} c_{ki}^{\cdot\cdot s} + c_{ks}^{\cdot\cdot p} c_{ij}^{\cdot\cdot s} = 0. \tag{19}$$

It can readily be seen that, conversely, if the numbers $c_{jk}^{\cdot\cdot i}$ satisfy relations (18) and (19) then we get an infinitesimal group on defining the operation of commutation by (17). Hence the consideration of the constants $c_{jk}^{\cdot\cdot i}$ which satisfy relations (18) and (19) is completely equivalent to the consideration of the infinitesimal group R.

THEOREM 66. *Let G be an r-dimensional Lie group. It follows from* B) *of* §38 *that to every differentiable curve $x(t)$ defined on G corresponds a tangent vector a. Hence the r-dimensional vector space R is associated with the group G. We establish in R the operation of commutation* (see Definition 46) *on the basis of the properties of the group G. Let a and b be two vectors in R, and let $x(t)$ and $y(t)$ be two curves to which the vectors a and b are tangent. Let*

$$q(t) = x(t)y(t)(x(t))^{-1}(y(t))^{-1}; \tag{20}$$

$q(t)$ then defines a curve in G. We introduce on this curve a new parameter s by letting $t = \sqrt{s}$. The new curve $q(\sqrt{s})$ thus defined for non-negative values of the parameter s has a tangent vector c, which is defined by the vectors a and b. We define the commutator $[a, b]$ by letting $[a, b] = c$. The operation of commutation thus defined in the space R satisfies conditions (14), (15), *and* (16). *The infinitesimal group R thus obtained is called the infinitesimal group of the Lie group G. The structural constants of the group G and of the infinitesimal group R coincide in corresponding coordinates* (see Definitions 45 and 46).

PROOF. To prove this we introduce in G a differentiable system of coordinates, and calculate the vector c in coordinate form. It can readily be seen that $c^i = \lim_{t\to 0} q^i(t)/t^2$. In view of (8) we have

$$c^i = \lim_{t\to 0} \frac{1}{t^2} (c_{jk}^{i} x^j(t) y^k(t) + \epsilon_2^i(t)) = c_{jk}^{i} a^j b^k,$$

where $\epsilon_2^i(t)$ is of the third order of magnitude with respect to t. In this way we have

$$c^i = [a, b]^i = c_{jk}^i a^j b^k.$$

Hence the structural constants of the infinitesimal group R coincide with the structural constants of the Lie group G. Since the structural constants of the group G satisfy relations (11) and (12), it follows that the commutators in R satisfy conditions (14), (15), and (16), i.e., R is really an infinitesimal group.

D) In order to calculate rapidly the commutators of the infinitesimal group R of the Lie group G we proceed as follows: let

$$q^{*i}(x, y) = q^{*i}(x^1, \cdots, x^r; y^1, \cdots, y^r)$$

be the sum of all the terms of the second order in the expansion of the difference $f^i(x, y) - f^i(y, x)$ (see (1)). Then the vector $c = [a, b]$ can be written in coordinate form as follows

$$c^i = q^{*i}(a^1, \cdots, a^r; b^1, \cdots, b^r). \tag{21}$$

The truth of this assertion follows directly from relation (9).

The part played by infinitesimal groups is explained by the fact that to every infinitesimal group corresponds uniquely some local Lie group. The following sections are devoted to the proof of this fact. The question of whether a complete Lie group corresponds to every infinitesimal group is a more difficult one, but it also can be solved in the affirmative. Of course uniqueness is not possible here, as to the same group R may correspond several non-isomorphic entire Lie groups, but all these Lie groups are locally isomorphic and the question of their connection follows from Schreier's results (see Chapter VIII).

Example 62. Let R be the three dimensional vector space in which the vector product is defined in the usual way: to every pair of vectors a and b corresponds their vector product $[a, b]$. If we now take for the commutator of the vectors a and b their vector product $[a, b]$, then the conditions of Definition 46 will follow from the usual rules of vector calculus. Hence we get an infinitesimal group R. It can be shown that to this infinitesimal group corresponds as a Lie group the group of rotations of the three dimensional Euclidean space around a fixed point.

Example 63. Let G be the multiplicative group of all square matrices of order n whose determinant is different from zero. In order to introduce coordinates into the group G, as should be done in a Lie group, we represent every matrix $x \varepsilon G$ in the form $x = e + x^*$, where e is the unit matrix. Then the elements of the matrix x^*, which we denote by x_j^i, can be taken as the coordinates of the element x. The dimension of the group G is therefore n^2. Under these conditions relations (4) can be written for the group G as follows:

$$f_j^i = x_j^i + y_j^i + x_k^i y_j^k. \tag{22}$$

We denote by R the infinitestimal group of the group G. We take for the

elements of the vector space R the totality of all square matrices of order n, having the usual rules of addition of matrices and multiplication by real numbers. If a and b are two matrices of the set R, then by remark D) and relation (22) the commutator is defined as follows:

$$c_j^i = [a, b]_j^i = a_k^i b_j^k - b_k^i a_j^k, \tag{23}$$

i.e.,

$$c = [a, b] = ab - ba. \tag{24}$$

The infinitesimal group R thus obtained is called the infinitesimal group of the group of all square matrices of order n. In order to visualize the elements of the set R as tangent vectors to curves in G, we consider a certain curve $x(t) = e + x^*(t)$ in G. The coordinates of the point $x(t)$ are the elements $x_j^i(t)$ of the matrix $x^*(t)$. The coordinates of the vector a tangent to the curve under consideration are the numbers $a_j^i = dx_j^i(0)/dt$. Hence the element $a \varepsilon R$ may be represented naturally in the form of the matrix $a = \|a_j^i\|$.

The matrix group G may be considered as a group of linear transformations of the n-dimensional vector space S. From this point of view every element $x \varepsilon G$ is merely a transformation $x(u)$ which associates with every vector $u \varepsilon S$ another vector $x(u) \varepsilon S$ in such a way that the condition of linearity holds, i.e.,

$$x(\alpha u + \beta v) = \alpha x(u) + \beta x(v),$$

where α and β are real numbers and u and v are vectors in S. The product f of two transformations x and y is defined as the transformation $f(u) = x(y(u))$.

The infinitesimal group R of the group G can now be composed from all linear mappings of the space G into itself. If a and b are two elements of R, then their sum d is defined by the relation $d(u) = a(u) + b(u)$, while the product of an element a by a real number α is given by $(\alpha a)(u) = \alpha a(u)$. It follows from (24) that the commutator $c = [a, b]$ is defined by

$$c(u) = a(b(u)) - b(a(u)), \tag{25}$$

i.e.,

$$[a, b] = ab - ba. \tag{26}$$

The above example of a matrix group plays an important part in the theory of Lie groups.

49. Subgroup. Factor Group. Homomorphic Mapping

In the previous section we associated with every Lie group G its infinitesimal group R. We construct here the infinitesimal group concepts which correspond to subgroup, normal subgroup, factor group and homomorphic mapping of the group G.

A) Let R be an infinitesimal group (see Definition 46). A set S of vectors

of the space R will be called an *infinitesimal subgroup* of the group R if the following conditions are fulfilled: a) the set S is a linear subspace of the space R, i.e., if a and b are vectors of S, then $\alpha a + \beta b$ is also a vector of S, where α and β are arbitrary real numbers. b) If a and b are two vectors of S, then the vector $[a, b]$ also belongs to S. An infinitesimal subgroup S of the infinitesimal group R is called a *normal subgroup,* if c) for $a \varepsilon R$, $b \varepsilon S$ we have $[a, b] \varepsilon S$. An infinitesimal subgroup S is called *central* if d) for $a \varepsilon R$, and $b \varepsilon S$ we have $[a, b] = 0$.

The following theorem justifies the terminology introduced in A).

THEOREM 67. *Let G be a local Lie group, R its infinitesimal group, and H a subgroup of the group G. We denote by S the set of all vectors which are tangent to curves in H* (see §38, B)). *Then S is a subgroup of the infinitesimal group R. We shall say that to the subgroup H corresponds the subgroup S, and denote this relation by $H \to S$. If H is a normal subgroup of the group G, then S is a normal subgroup of the group R. If H is a central normal subgroup of the group G, then S is a central normal subgroup of the group R.*

PROOF. By Theorem 50, H is a differentiable sub-manifold of the manifold G, and therefore S is a linear subspace of the space R. Hence condition a) of definition A) is satisfied. We shall show that condition b) is also satisfied. Let a and b be two vectors of S, and let $x(t)$ and $y(t)$ be two curves in H to which the vectors a and b are tangent. In order to find the vector $c = [a, b]$ we consider the curve $q(t) = x(t)y(t)(x(t))^{-1}(y(t))^{-1}$ (see Theorem 66). This curve is also in H, since H is a group. Hence the curve $q(\sqrt{s})$ is in H, and therefore the vector c which is tangent to the curve $q(\sqrt{s})$ is in S, and we have $[a, b] \varepsilon S$.

We shall prove relation c) of definition A) in case H is a normal subgroup of the group G. Let $a \varepsilon R$, and $b \varepsilon S$. We denote by $x(t)$ a curve of G with the tangent vector a, and by $y(t)$ a curve of H with the tangent vector b. The element $x(t)y(t)(x(t))^{-1}$ belongs to H, since H is a normal subgroup. Therefore the element $q(t) = x(t)y(t)(x(t))^{-1}(y(t))^{-1}$ also belongs to H. Hence the curve $q(\sqrt{s})$ is in H and its tangent vector $c = [a, b]$ belongs to S.

In order to consider the case in which H is a central normal subgroup we continue our discussion of normal subgroups. In this case $q(t)$ can easily be seen to degenerate into the point e and therefore the tangent vector c is a null vector. This proves Theorem 67.

B) Let R be an infinitesimal group and S a normal subgroup of R (see A)). We divide the vector group R into cosets of the subgroup S. The set R^* of cosets thus obtained is in turn a vector space. The operation of commutation can easily be introduced into the space R^* (see Definition 46). Let A and B be two cosets. Furthermore let $a \varepsilon A$ and $b \varepsilon B$, and let $c = [a, b]$. We shall show that the coset C containing the element c does not depend on the choice of the elements a and b, but is defined by the cosets A and B. To prove this we take an arbitrary element $a' \varepsilon A$ and show that $c' = [a', b] \varepsilon C$. In fact

$c' - c = [a', b] - [a, b] = [a' - a, b] \in S$ (see A), c)). Hence $c' \in C$. The commutator $[A, B]$ of the elements A and B is defined by letting $[A, B] = C$. Since the operation of commutation in R satisfies conditions (14), (15), and (16) of §48, it is not hard to show that the same conditions hold in R^*. In this way R^* is an infinitesimal group. R^* is called the *factor group* of the infinitesimal group R by its normal divisor S. In symbols, $R^* = R/S$.

C) Let R and R' be two infinitesimal groups and let g be a mapping of R on R'. The mapping g is called *homomorphic* if the following conditions hold: a) the mapping g is linear, i.e., we have for arbitrary real numbers α and β,

$$g(\alpha a + \beta b) = \alpha g(a) + \beta g(b) \quad \text{where} \quad a \in R,\ b \in R,$$

and b) $g([a, b]) = [g(a), g(b)]$, where $a \in R$, $b \in R$. The set S of all the elements of R which go into the zero of R' under g is called the *kernel* of the homomorphism g. A homomorphic mapping is called *isomorphic* if it is one-to-one. Two infinitesimal groups R and R' are called *isomorphic* if there exists an isomorphic mapping of one group onto the other.

D) Let R and R' be two infinitesimal groups and let g be a homomorphic mapping of the group R on R'. We denote by S the set of all elements of the group R which map into the zero of the group R' under the homomorphism g. Then S is a normal subgroup of the infinitesimal group R, and the factor group R/S is isomorphic with the group R' (see A), B) and C)).

Since g is a linear mapping of the space R on the space R' it follows that S is a linear subspace of the space R. Let $a \in R$, $b \in S$. Then

$$g[a, b]) = [g(a), g(b)] = [g(a), 0] = 0.$$

Hence $[a, b] \in S$, i.e., S is a normal subgroup of the infinitesimal group R.

Now let a' be an element of R'. We denote by A the set of all elements of R which go into a' under the mapping g. Since g is a homomorphic mapping of the vector group R on the vector group R', it follows from the general theorems about the homomorphism of groups that A is a coset of S. In this way there exists a one-to-one correspondence between the elements of the factor group R/S and the elements of the group R'. The proof of the fact that this correspondence establishes an isomorphism between the infinitesimal groups R/S and R' is quite trivial.

The following theorem justifies the concepts which we have introduced here.

THEOREM 68. *Let G and G' be two local Lie groups and let f be a locally homomorphic mapping of the group G on the group G'. We denote by R and R' the infinitesimal groups of the groups G and G'. Let $a \in R$, and let $x(t)$ be a curve in G having the vector a for tangent. The function $f(x(t))$ defines a curve in G' whose tangent vector we denote by a'. Then the vector a' is defined by the vector a, i.e., it does not depend on the choice of the curve $x(t)$, except that it must have the tangent vector a. Therefore we can write $a' = g(a)$, where g is a homomorphic mapping of the infinitesimal group R on the infinitesimal group R'.*

In this way to every homomorphism f of the group G on the group G' corresponds a homomorphism g of their infinitesimal groups, $f \to g$. We denote by N the kernel of the homomorphism f, and by S the kernel of the homomorphism g. Then to the subgroup N of the group G corresponds the subgroup S of the infinitesimal group R, $N \to S$ (see Theorem 67).

PROOF. By Theorem 51 the mapping f can be expressed by means of differentiable functions. This means that the mapping g defined in the theorem is uniquely determined, and is a linear mapping of the space R on the space R'. Let $x(t)$ and $y(t)$ be two curves in G, and let a and b be the vectors tangent to them. Let

$$q(t) = x(t)y(t)(x(t))^{-1}(y(t))^{-1}.$$

Then the vector $c = [a, b]$ is a tangent to the curve $q(\sqrt{s})$ (see Theorem 66). The vectors $a' = g(a)$ and $b' = g(b)$ are tangent to the curves $x'(t) = f(x(t))$ and $y'(t) = f(y(t))$. In order to define the vector $c' \doteq [a', b']$ we consider the curve

$$q'(t) = x'(t)y'(t)(x'(t))^{-1}(y'(t))^{-1}.$$

Since the mapping f is homomorphic, it follows that $q'(\sqrt{s}) = f(q(\sqrt{s}))$. Hence $g(c) = c'$ and the homomorphism of the mapping g is established.

We denote by S' that infinitesimal subgroup which corresponds to the subgroup N (see Theorem 67). Since every curve of N goes over into the point e' under the homomorphism f, $S' \subset S$. The equality $S' = S$ follows from the calculation of their dimensions. This proves Theorem 68.

E) Let G, G', and G'' be three local Lie groups and R, R', and R'' their infinitesimal groups. Suppose we have defined local homomorphisms f' and f'' of the group G on the group G' and of the group G' on the group G''. The corresponding homomorphisms of the infinitesimal groups we denote by g' and g'', $f' \to g'$, and $f'' \to g''$ (see Theorem 68). Let $f(x) = f''(f'(x))$ and $g(a) = g''(g'(a))$. Then to the homomorphism f corresponds the homomorphism g, i.e., $f \to g$.

The proof of proposition E) follows directly from the definition of the correspondence given in Theorem 68. If $x(t)$ is a curve of G having the tangent vector a, then the curve $f'(x(t))$ has the tangent vector $g'(a)$, and hence the curve $f''(f'(x(t)))$ has the tangent vector $g''(g'(a))$. It follows that the curve $f(x(t))$ has the tangent vector $g(a)$ and therefore, $f \to g$.

Theorems 67 and 68 show that to every concept or relation concerning Lie groups corresponds naturally and uniquely some concept or relation for infinitesimal groups. To the inverse transition from infinitesimal to Lie groups we shall devote the following section.

It would not be hard to introduce the concept of direct product for infinitesimal groups and to show that to the decomposition into a direct product of a local Lie group corresponds a decomposition into a direct product of its infini-

tesimal group. However, because of the complete triviality of the construction, I shall not stop to carry it out.

EXAMPLE 64. We continue the discussion of Example 62, and show that the infinitesimal group R of that example has one-dimensional subgroups only, and that every one-dimensional linear subspace of the infinitesimal group is a subgroup of it. Let us suppose that R admits a two-dimensional subgroup S. Then S contains two linearly independent vectors a and b. The vector $[a, b] = c$, which is the vector product of a and b, will be distinct from zero and perpendicular to the plane S. Hence c cannot be contained in S. In the same way it can be verified that the group R is simple, i.e., it has no non-trivial normal subgroups.

EXAMPLE 65. Let us continue the discussion of Example 63 by selecting some interesting subgroups of the group G given in that example, and finding which subgroups of the infinitesimal group R correspond to them.

Let H be the subgroup composed of all matrices whose determinant is equal to unity. We consider an arbitrary curve $x(t)$ in H. The determinant of the matrix $x(t)$ is equal to unity. It is not hard to see that in coordinate form it is of the type $1 + x_i^i(t) + \epsilon_7(t)$, where $\epsilon_7(t)$ is a quantity of the second order of magnitude with respect to t (here as usual we suppose that summation is carried out with respect to the index i). Since this determinant must be equal to unity, it follows that $dx_i^i(0)/dt = 0$. Hence the vector a which is tangent to the curve $x(t)$ satisfies the condition which can be written in coordinate form

$$a_i^i = 0, \tag{1}$$

i.e., the trace of the matrix a is equal to zero. We denote by A that subgroup of the group R which corresponds to the subgroup H (see Theorem 67). Every matrix of A satisfies condition (1). The converse is also true and follows from the fact that the dimension of H is equal to $n^2 - 1$, and hence the dimension of A is also $n^2 - 1$, and therefore A must contain all the matrices which satisfy condition (1).

Let K be the subgroup of all orthogonal matrices (see Example 4) and B the subgroup of the infinitesimal group R which corresponds to it. In considering orthogonal matrices it is more convenient to write both indices of the elements as subscripts. Let $x(t)$ be a curve in K. Then this curve $x(t)$ satisfies in coordinate form the following condition

$$\delta_{ij} + x_{ij}(t) + x_{ji}(t) + \sum_{k=1}^{n} x_{ik}(t)x_{jk}(t) = \delta_{ij}.$$

Taking derivatives with respect to t on both sides of this equation we get the following conditions for the tangent vector a to the curve $x(t)$:

$$a_{ij} + a_{ji} = 0. \tag{2}$$

Hence B is composed of skew symmetric matrices.

50. Integrability Conditions

In constructing Lie groups by means of their structural constants we make use of one elementary result in the theory of partial differential equations. We here give this result without proof, and derive from it some conclusions which will be of use later.

We consider the system of differential equations

$$\frac{\partial f^i}{\partial x^j} = \varphi^i_j(f^1, \cdots, f^n; x^1, \cdots, x^r) = \varphi^i_j(f, x) \qquad i = 1, \cdots, n; j = 1, \cdots, r. \tag{1}$$

where f is a point with coordinates $f^1, \cdots, f^n$, and x a point with coordinates $x^1, \cdots, x^r$. The functions $\varphi^i_j(f, x)$ are defined and are doubly differentiable or even analytic in the region of values of $f \varepsilon U$ and $x \varepsilon V$, where U and V are open sets in the corresponding coordinate spaces, while $x^1, \cdots, x^r$ are independent variables, and $f^1, \cdots, f^n$ are functions of these variables. We have to find a function $f(x)$, or in coordinate form, a system of functions

$$f^i(x) = f^i(x^1, \cdots, x^r), \qquad i = 1, \cdots, n,$$

which are such that conditions (1) are identically true in the independent variables $x^1, \cdots, x^r$.

A natural way of proposing the question of solving the system (1) is as follows. Let the initial conditions $x_0 \varepsilon V, f_0 \varepsilon U$ be given. It is required to find a solution $f(x)$ such that

$$f(x_0) = f_0, \tag{2}$$

where $f(x)$ must be differentiable and defined for values of the argument x in the neighborhood of x_0. Then the following theorem holds.

THEOREM 69. *In order that the system* (1) *should have a solution for arbitrary initial values* $x_0 \varepsilon V$, *and* $f_0 \varepsilon U$, *it is necessary that the following relation be identically true*

$$\frac{\partial \varphi^i_k(f, x)}{\partial f^\alpha} \varphi^\alpha_j(f, x) + \frac{\partial \varphi^i_k(f, x)}{\partial x^j} - \frac{\partial \varphi^i_j(f, x)}{\partial f^\alpha} \varphi^\alpha_k(f, x) - \frac{\partial \varphi^i_j(f, x)}{\partial x^k} = 0 \tag{3}$$

for all values of $x \varepsilon V, f \varepsilon U$. *On the other hand if relation* (3) *holds for all values of* $x \varepsilon V, f \varepsilon U$, *then there exists a unique solution* $f(x)$ *with arbitrary initial conditions* $x_0 \varepsilon V, f_0 \varepsilon U$.

We express the dependence of the solution $f(x)$ on its initial conditions by writing $f(x) = f(x, f_0, x_0)$. Let U' and V' be two open sets having compact closures $\bar{U}'$ and V' such that $\bar{U}' \subset U$ and $\bar{V}' \subset V$. Then it is possible to find a sufficiently small positive number ϵ such that for $f_0 \varepsilon U'$, $x_0 \varepsilon V'$ and $|x^i - x^i_0| < \epsilon$, $i = 1, \cdots, r$, the solution $f(x, f_0, x_0)$ exists and is triply differ-

entiable (or even correspondingly analytic) with respect to all the arguments x, f_0, x_0.

Relations (3) are called the *integrability conditions* for the system (1). I prove here only the necessity of conditions (3).*

Suppose that there exists a solution $f(x)$ of the system (1) with arbitrary initial conditions $x_0 \varepsilon V$, $f_0 \varepsilon U$. We substitute the solution $f(x)$ into the system (1), and differentiating the resulting identity, we get

$$(4) \qquad \frac{\partial^2 f^i}{\partial x^j \partial x^k} = \frac{\partial \varphi_j^i(f, x)}{\partial f^\alpha}\frac{\partial f^\alpha}{\partial x^k} + \frac{\partial \varphi_j^i(f, x)}{\partial x^k} = \frac{\partial \varphi_j^i(f, x)}{\partial f^\alpha}\overset{\alpha}{\varphi}_k(f, x) + \frac{\partial \varphi_j^i(f, x)}{\partial x^k}.$$

Since

$$\frac{\partial^2 f^i}{\partial x^j \partial x^k} = \frac{\partial^2 f^i}{\partial x^k \partial x^j},$$

relation (3) holds for $f = f(x)$.

For $x = x_0$ we have $f(x_0) = f_0$ and therefore relation (3) holds for $x = x_0$, $f = f_0$. Since, by assumption, the initial values may be assigned arbitrarily, equation (3) holds for arbitrary $x \varepsilon V$, $f \varepsilon U$. Hence the necessity of condition (3) is established.

In what follows we shall not be concerned directly with a system of the type (1), but with a system in which the derivatives $\partial f^i/\partial x^j$ are not given explicitly. We shall therefore write the integrability conditions for the system of equations which will concern us in a form more desirable for our purposes.

A) We consider the system of differential equations

$$(5) \qquad \overset{i}{v}_k(f)\frac{\partial f^k}{\partial x^j} = \overset{i}{v}_j(x), \quad i = 1, \cdots, r; j = 1, \cdots, r$$

where $v_j^i(z) = v_j^i(z^1, \cdots, z^r)$ are functions which are defined and are doubly differentiable in the region $z \varepsilon U$, and are such that the determinant of the matrix $\|v_j^i(z)\|$ does not become zero in this region. The system (5) can easily be reduced to the form (1), and therefore its integrability conditions can be written as

$$(6) \qquad \frac{\partial \overset{i}{v}_k(z)}{\partial z^j} - \frac{\partial \overset{i}{v}_j(z)}{\partial z^k} = \tilde{c}^{\,i}_{\alpha\beta}\overset{\alpha}{v}_j(z)\overset{\beta}{v}_k(z),$$

where $\tilde{c}^i_{jk}$ are certain constants. The system (5) can be rewritten in the following symmetric form

$$(7) \qquad \overset{i}{v}_j(f)\partial f^j = \overset{i}{v}_j(x)\partial x^j,$$

where ∂f^j is the total derivative of the function $f^j(x)$, and ∂x^j is the derivative with respect to the independent variable x^j.

* For a proof of the sufficiency see de la Vallée-Poussin, Cours d'Analyse, vol. 2, chapter on equations in total differentials.

In order to deduce relation (6) we introduce the matrix $\|u^i_j(z)\|$ inverse to the matrix $\|v^i_j(z)\|$. This matrix exists since the determinant of the matrix $\|v^i_j(z)\|$ is, by assumption, distinct from zero in the region U. We have

$$u^i_\alpha(z)v^\alpha_j(z) = v^i_\alpha(z)u^\alpha_j(z) = \delta^i_j, \tag{8}$$

where $\|\delta^i_j\|$ is the unit matrix. Differentiating relation (8) we get

$$v^i_\alpha(z)\frac{\partial u^\alpha_j(z)}{\partial z^k} + \frac{\partial v^i_\alpha(z)}{\partial z^k}u^\alpha_j(z) = 0. \tag{9}$$

Multiplying (5) by $u^p_i(f)$ and summing over i we get, changing the notation of the indices,

$$\frac{\partial f^i}{\partial x^j} = u^i_\beta(f)v^\beta_j(x). \tag{10}$$

In this way the system (5) is reduced to the form (1), and Theorem 69 is therefore applicable to it. By this theorem the integrability condition for the system (10) has the form

$$\frac{\partial u^i_\beta(f)}{\partial f^\alpha}u^\alpha_\gamma(f)v^\gamma_j(x)v^\beta_k(x) + u^i_\beta(f)\frac{\partial v^\beta_k(x)}{\partial x^j} - \frac{\partial u^i_\beta(f)}{\partial f^\alpha}u^\alpha_\gamma(f)v^\gamma_k(v)v^\beta_j(x) - u^i_\beta(f)\frac{\partial v^\beta_j(x)}{\partial x^k} = 0. \tag{11}$$

Multiplying (11) by $v^p_i(f)$ and summing over i we get from (9) and (8)

$$-\frac{\partial v^p_i(f)}{\partial f^\alpha}u^i_\beta(f)u^\alpha_\gamma(f)v^\gamma_j(x)v^\beta_k(x) + \frac{\partial v^p_k(x)}{\partial x^j} + \frac{\partial v^p_i(f)}{\partial f^\alpha}u^i_\beta(f)u^\alpha_\gamma(f)v^\gamma_k(x)v^\beta_j(x) - \frac{\partial v^p_j(x)}{\partial x^k} = 0.$$

Multiplying the last relation by $u^j_s(x)u^k_t(x)$ and summing over j and k we get

$$\left(\frac{\partial v^p_\beta(x)}{\partial x^\alpha} - \frac{\partial v^p_\alpha(x)}{\partial x_\beta}\right)u^\alpha_s(x)u^\beta_t(x) = \left(\frac{\partial v^p_\beta(f)}{\partial f^\alpha} - \frac{\partial v^p_\alpha(f)}{\partial f^\beta}\right)u^\alpha_s(f)u^\beta_t(f). \tag{12}$$

The last relation must be true identically. Since the variables are separated in it, each side of it must be a constant. Hence we have

$$\left(\frac{\partial v^i_\beta(z)}{\partial z^\alpha} - \frac{\partial v^i_\alpha(z)}{\partial z^\beta}\right)u^\alpha_s(z)u^\beta_t(z) = \tilde{c}^i_{st}.$$

Multiplying this last relation by $v^s_j(z)v^t_k(z)$ and summing over s and t we get relation (6). Proceeding in the opposite direction we can get relation (11) from relation (6).

51. The Construction of Lie Groups from Structural Constants

We shall give here a construction of a local Lie group by means of its structural constants. This construction will be carried out in terms of coordinates, i.e. we shall endeavor to find functions $f^i(x, y)$ which express the coordinates of the element $f = xy = f(x, y)$ in terms of the coordinates of the elements x and y (see Definition 45). It is evident that the structural constants themselves cannot define the functions $f^i(x, y)$, since there exist transformations of coordinates which do not change the structural constants but do change these functions. Therefore, we must select for this construction some special coordinates, such as the canonical coordinates of the first or second kind. Either of these choices is possible. We make use here of the canonical coordinates of the first kind. The construction of a local Lie group is carried out in two steps. The first step consists in the introduction of some auxiliary functions which define uniquely the functions $f^i(x, y)$, and are themselves defined by the latter. These auxiliary functions satisfy certain differential equations which contain the structural constants. The second step consists in the solution of these equations. It is necessary here to use canonical coordinates because the auxiliary functions are uniquely defined by the structural constants only in these coordinates.

A) Let G be a local Lie group and let

$$f = xy = f(x, y). \tag{1}$$

This relation may be written in coordinate form as follows:

$$f^i = f^i(x, y) = f^i(x^1, \cdots, x^r; y^1, \cdots, y^r). \tag{2}$$

We shall now introduce the auxiliary functions. We denote symbolically by $x + \delta x$ the element whose coordinates are $x^i + \delta x^i$, $i = 1, \cdots, r$, where x^i, $i = 1, \cdots, r$, are the coordinates of a certain element x, while

$$\delta x^i, \qquad i = 1, \cdots, r, \tag{3}$$

are small increments.

Let $p = (x + \delta x)x^{-1}$, and let us expand the coordinates of the element p in Taylor series in powers of the increments (3). We then have

$$\overset{i}{p} = \overset{i}{v}_j(x)\delta \overset{j}{x} + \overset{i}{\epsilon}_1, \tag{4}$$

where ϵ_1^i is of the second order of magnitude with respect to the increments (3), while $v_j^i(x) = v_j^i(x^1, \cdots, x^r)$ is a function of x. In this notation the following relation holds:

$$\overset{i}{v}_j(e) = \overset{i}{\delta}_j, \tag{5}$$

where $\|\delta_j^i\|$ is the unit matrix, and e is the identity of the group G. Also

$$\overset{i}{v}_k(f)\frac{\partial f^k}{\partial x^j} = \overset{i}{v}_j(x). \tag{6}$$

Hence $f(x, y)$, as a function of x, (for y constant) satisfies the system of differential equations (6) with the obvious initial conditions

(7) $$f(e, y) = y.$$

Finally the funticons $v_j^i(x)$ satisfy the following system of equations

(8) $$\frac{\partial v_k^i(x)}{\partial x^j} - \frac{\partial v_j^i(x)}{\partial x^k} = c_{\alpha\beta}^i v_j^\alpha(x) v_k^\beta(x)$$

where c_{jk}^i are the structural constants of the group G. It is worth noting that relation (8) is nothing else but the integrability condition for the system (6) (see §50, A)).

We also note that it is possible to write the equation of a one parameter subgroup in a simple form by making use of the auxiliary functions $v_j^i(x)$. In fact, if $x(t)$ is a one-parameter subgroup of the group G, having the direction vector a, then the following relation holds:

(9) $$a^i = v_j^i(x(t)) \frac{dx^j(t)}{dt} \cdot$$

Relation (5) is obvious. To prove (6) we assign in (1) certain increments to the coordinates of the element x. Then the coordinates of the element f also acquire certain increments, and we have

$$f + \delta f = (x + \delta x)y.$$

It follows from this and from (1) that

$$(f + \delta f)f^{-1} = (x + \delta x)y(xy)^{-1} = (x + \delta x)x^{-1}.$$

This last relation can be written in coordinate form by making use of (4) as follows:

(10) $$v_k^i(f)\delta f^k = v_j^i(x)\delta x^j + \epsilon_2^i,$$

where ϵ_2^i is of the second order of magnitude with respect to the increments (3). Expanding the functions δf^k in a Taylor series in powers of the increments (3) we get

(11) $$\delta f^k = \frac{\partial f^k}{\partial x^j} \delta x^j + \epsilon_3^i,$$

where ϵ_3^i is of the second order of magnitude. It follows from relations (10) and (11) that

$$v_k^i(f) \frac{\partial f^k}{\partial x^j} \delta x^j = v_j^i(x)\delta x^j + \epsilon_4^i.$$

By comparing the coefficients in this last relation we obtain (6)

In order to prove (8) we note that if x_0 and f_0 are two elements in the neighborhood of the identity, then there exists an element y_0 such that $f_0 = x_0 y_0$. Hence the system (6) has a solution for arbitrary initial conditions x_0 and f_0 in the neighborhood of the identity e. Hence by Theorem 69, the integrability conditions hold for the system (6). By remark A) of §50, these integrability conditions have the form

$$\frac{\partial \overset{i}{v}_k(x)}{\partial x^j} - \frac{\partial \overset{i}{v}_j(x)}{\partial x^k} = \tilde{c}^{\,i}_{\alpha\beta} \overset{\alpha}{v}_j(x) \overset{\beta}{v}_k(x), \tag{12}$$

where $\tilde{c}^{\,i}_{jk}$ are certain constants. It remains to show that these constants are the structural constants of the group G. For $x = e$, relation (6) gives

$$\overset{i}{v}_\alpha(y) \frac{\partial f^\alpha(e, y)}{\partial x^j} = \delta^i_j.$$

Differentiating this last equation we get

$$\frac{\partial \overset{i}{v}_\alpha(y)}{\partial y^k} \frac{\partial f^\alpha(e, y)}{\partial x^j} + \overset{i}{v}_\alpha(y) \frac{\partial^2 f^\alpha(e, y)}{\partial x^j \partial y^k} = 0,$$

which becomes for $y = e$

$$\frac{\partial \overset{i}{v}_j(e)}{\partial y^k} + \frac{\partial^2 f^i(e, e)}{\partial x^j \partial y^k} = 0. \tag{13}$$

It follows from here and from (4) of §48 that $\partial \overset{i}{v}_j(e)/\partial y^k = -\, a^i_{jk}$. Hence for $x = e$, relation (12) becomes

$$\overset{i}{a}_{jk} - \overset{i}{a}_{kj} = \tilde{c}^{\,i}_{jk},$$

i.e., the $\tilde{c}^{\,i}_{jk}$ are the structural constants of the group G (see §48, (5)).

To prove (9) we let the parameter t have a small increment δt. Then we have

$$x(t + \delta t)(x(t))^{-1} = x(\delta t),$$

and therefore

$$x^i(\delta t) = \overset{i}{v}_j(x(t))(x^j(t + \delta t) - x^j(t)) + \overset{i}{\epsilon}_1.$$

Dividing both sides of this equation by δt and passing to the limit as $\delta t \to 0$, we obtain relation (9). Hence A) is completely established.

THEOREM 70. *Let U be an open set of the r-dimensional Euclidean space containing the origin of coordinates e. Suppose the following doubly differentiable functions are defined in U:*

$$\overset{*}{v}{}^i_j(x) = \overset{*}{v}{}^i_j(x^1, \cdots, x^r),$$

such that the determinant of the matrix $\|\overset{*}{v}{}^i_j(x)\|$ *does not become zero in the region* U, *and such that the following conditions are satisfied.*

(14) $$\overset{*}{v}{}^i_j(e) = \delta^i_j$$

(15) $$\frac{\partial \overset{*}{v}{}^i_k(x)}{\partial x^j} - \frac{\partial \overset{*}{v}{}^i_j(x)}{\partial x^k} = \overset{*}{c}{}^i_{\alpha\beta}\overset{*}{v}{}^\alpha_j(x)\overset{*}{v}{}^\beta_k(x)$$

where $\overset{*}{c}{}^i_{jk}$ *are certain constants. We form the system of differential equations*

(16) $$\overset{*}{v}{}^i_k(f)\frac{\partial f^k}{\partial x^j} = \overset{*}{v}{}^i_j(x).$$

Relations (15) *are the integrability conditions for the system* (16) (see §50, A)), *and therefore by Theorem* 69 *there exists a neighborhood* G *of the origin of coordinates* e *such that, for any* $x_0 \varepsilon G$ *and* $f_0 \varepsilon G$, *there exists a solution* $f(x, f_0, x_0)$ *having the initial values* x_0 *and* f_0 *which holds for all* $x \varepsilon G$. *Let* $f(x, y) = f(x, y, e)$. *Then*

(17) $$f(e, y) = y.$$

We now define the law of multiplication of two points x *and* y *by setting*

(18) $$f = xy = f(x, y).$$

Then with this law of multiplication G *is a local Lie group such that the auxiliary functions* $v^i_j(x)$ *of the group* G (see A)) *coincide with the given functions* $\overset{*}{v}{}^i_j(x)$ *and the structural constants* c^i_{jk} *of the group* G *coincide with the constants* $\overset{*}{c}{}^i_{jk}$, *i.e.,*

(19) $$v^i_j(x) = \overset{*}{v}{}^i_j(x)$$

(20) $$c^i_{jk} = \overset{*}{c}{}^i_{jk}.$$

Proof. We prove first of all the associativity of the multiplication law. It follows from (17) that $f(e, e) = e$. Since the function $f(x, y)$ is continuous, we can select a sufficiently small neighborhood V of the point e such that for $x \varepsilon V$, $y \varepsilon V$ we have $f(x, y) \varepsilon G$. Let $x \varepsilon V$, $y \varepsilon V$, $z \varepsilon V$, and let $u = f(x, y)$, $v = f(y, z)$, $w = f(u, z)$, $w^* = f(x, v)$. We shall then show that $w = w^*$, which will prove associativity.

In this proof we shall consider the elements y and z as fixed, and x as variable. From the definition of the function f, the function $w^*(x)$ is a solution of the system (16) with the initial condition $w^*(e) = v$. We shall show that $w(x)$ is also a solution of the system (16) with the same initial condition $w(e) = v$. Because of the uniqueness of the solution of the system (16) (see Theorem 69), it will follow that $w^*(x) = w(x)$.

We have for $x = e$ that $u = y$, i.e., $w = f(y, z) = v$. Hence the initial conditions coincide for the functions $w(x)$ and $w^*(x)$.

In order to show that $w(x)$ is a solution of the system (16) we introduce the

matrix $\|u_j^{*i}(x)\|$ inverse to the matrix $\|v_j^{*i}(x)\|$. In this notation the system (16) may be written

(21) $$\frac{\partial f^i}{\partial x^j} = \overset{*}{u}{}_k^i(f)\overset{*}{v}{}_j^k(x).$$

Furthermore, we have

$$\frac{\partial w^i}{\partial x^j} = \frac{\partial w^i}{\partial u^\alpha}\cdot\frac{\partial u^\alpha}{\partial x^j} = \overset{*}{u}{}_k^i(w)\overset{*}{v}{}_\alpha^k(u)\overset{*}{u}{}_l^\alpha(u)\overset{*}{v}{}_j^l(x) = \overset{*}{u}{}_k^i(w)\overset{*}{v}{}_j^k(x).$$

Hence $w(x)$ is a solution of the system (21) and associativity is proved.

The identity of the group G is the element e. For $f = x$, as can easily be seen, is a solution of the system (16) with the initial condition $f(e) = e$. Hence, because of the uniqueness of the solution, $f(x, e) = x$, i.e., $xe = x$.

In order to find the inverse element, it is necessary to solve with respect to y the system of equations

(22) $$f^i(x, y) = 0.$$

For $x = e$ this system has the obvious solution $y = e$. Furthermore it follows from relation (17) that the Jacobian of the system (22) is equal to unity for $x = y = e$. Hence the system (22) is solvable for y in the neighborhood of the identity e, and the existence of the inverse element is proved.

Since we have already shown that G is a local Lie group, it follows from remark A) that the function $f(x, y)$ satisfies the system (6) and at the same time the system (16). It follows from this that $v_j^i(z) = v_j^{*i}(z)$, since by putting $x = e$ in the systems (6) and (16) we get a method of calculating the functions $v_j^i(z)$ and $v_j^{*i}(z)$ by means of $f(x, y)$ (see (5) and (14)). By (19) the constants of equations (8) and (15) must coincide, i.e., $c_{jk}^i = c_{jk}^{*i}$. This proves Theorem 70.

The first step in the construction of a Lie group is now completed. We pass to the second step. Here the problem consists in solving the system (8), i.e., in finding the auxiliary functions $v_j^i(x)$ from the structural constants. The form of the system (8) shows that the solution satisfying the initial conditions (5) is not uniquely defined. As already mentioned, it is necessary to specialize in some way the choice of coordinates in order to impose an additional condition on the functions $v_j^i(x)$ and solve the problem uniquely. We chose as these special coordinates the canonical coordinates of the first kind (see §39, B)).

The problem of solving the system (3) in canonical coordinates can be reduced to the integration of a system of ordinary differential equations. The method used here is a rather common one. The functions $v_j^i(x)$ are not sought at once in the whole neighborhood of the identity, but along a certain curve, in this case along a one-parameter subgroup. If $g(t)$ is a one-parameter subgroup, we have, in view of our canonical coordinates, $g^i(t) = a^it$. The functions $v_j^i(g(t))$ for a fixed subgroup $g(t)$ depend on a single parameter t. It turns out that the functions $tv_j^i(g(t))$, as functions of the parameter t, satisfy a certain system of ordinary linear differential equations with constant coefficients.

The solution of these equations is reduced to a simple application of an elementary existence theorem, and the problem is completely solved.

We give here one characteristic property of the system of canonical coordinates of the first kind.

B) Let D be a system of coordinates in a local Lie group. In order that the system D be canonical of the first kind it is necessary and sufficient that there exist auxiliary functions $v^i_j(x)$ in the system D (see A)) which satisfy the following relation:

$$v^i_j(x)x^j = x^i. \tag{23}$$

Suppose that the coordinates D are canonical of the first kind. Let $g(t)$ be a one-parameter subgroup of the group D having the direction vector a (see §39, A)). Since the coordinates D are canonical we have $g^i(t) = a^i t$. Making use of (9) we have

$$v^i_j(at)a^j = a^i. \tag{24}$$

This relation becomes (23) for $a = x$, $t = 1$.

Suppose now that relation (23) holds. Let $g(t)$ be a one-parameter subgroup having the direction vector a. From relation (9) we have

$$v^i_j(g(t))\,\frac{dg^j(t)}{dt} = a^i. \tag{25}$$

In view of relation (23), the system (25) is satisfied for $g^i(t) = a^i t$. Hence, because of the uniqueness of the solution of the system (25), we have $g^i(t) = a^i t$, i.e., the system of coordinates D is canonical of the first kind.

C) Let G be a local Lie group and D a canonical system of coordinates of the first kind defined in it. Further, let $v^i_j(x) = v^i_j(x^1, \cdots, x^r)$ be the auxiliary functions (see A)) defined in the system D. Let

$$w^i_j(t) = w^i_j(t, a) = tv^i_j(a^1 t, \cdots, a^r t) = tv^i_j(at), \tag{26}$$

where a is a fixed vector, and at represents symbolically a vector with coordinates $a^i t$: this notation is not common, but it is natural in canonical coordinates of the first kind. Then the following relations hold

$$v^i_j(x) = w^i_j(1, x), \tag{27}$$

$$w^i_j(0, a) = 0, \tag{28}$$

$$\frac{dw^i_j(t)}{dt} = \delta^i_j + c^i_{\alpha\beta}a^\alpha w^\beta_j(t). \tag{29}$$

In this way the functions $w^i_j(t, a)$, considered as functions of the parameter t, are solutions of the system (29) with initial conditions (28). From the functions $w^i_j(t, a)$ we can now define by means of relation (27) the desired functions $v^i_j(x)$. This will show that in canonical coordinates of the first kind the auxiliary functions $v^i_j(x)$ are uniquely defined by the structural constants c^i_{jk}.

Relations (27) and (28) are obvious. We shall now prove relation (29). Differentiating (23) we get

$$\frac{x^k \partial v^i_k(x)}{\partial x^j} + v^i_j(x) = \delta^i_j. \tag{30}$$

Multiplying (8) by x^k and summing over k we get

$$\frac{\partial v^i_k(x)}{\partial x^j} x^k - \frac{\partial v^i_j(x)}{\partial x^k} x^k = c^i_{\alpha\beta} v^\alpha_j(x) v^\beta_k(x) x^k = - c^i_{\alpha\beta} x^\alpha v^\beta_j(x) \tag{31}$$

(see (23) and §48, (6)). From relations (30) and (31) it follows that

$$\frac{\partial v^i_j(x)}{\partial x^k} x^k + v^i_j(x) = \delta^i_j + c^i_{\alpha\beta} x^\alpha v^\beta_j(x)$$

Replacing x by at in the last relation we get

$$\frac{\partial v^i_j(at)}{\partial x^k} ta^k + v^i_j(at) = \delta^i_j + c^i_{\alpha\beta} a^\alpha t v^\beta_j(at). \tag{32}$$

The left side of the last relation can easily be seen to be the derivative of the function $w^i_j(t, a)$ with respect to t. Hence relation (32) can be written in the form (29).

THEOREM 71. *Let c^{*i}_{jk} be a system of constants satisfying the following relations*

$$c^{*i}_{jk} = - c^{*i}_{kj}, \tag{33}$$

$$c^{*p}_{is} c^{*s}_{jk} + c^{*p}_{js} c^{*s}_{ki} + c^{*p}_{ks} c^{*s}_{ij} = 0. \tag{34}$$

We consider the system of ordinary differential equations

$$\frac{dw^{*i}_j}{dt} = \delta^i_j + c^{*i}_{\alpha\beta} a^\alpha w^{*\beta}_j, \tag{35}$$

where a is a constant vector, and w^{*i}_j are unknown functions of the parameter t. The system (35) is linear with constant coefficients, and therefore its solutions exist for all values of t, $-\infty < t < \infty$. We denote by $w^{*i}_j(t, a)$ the solution of the system (35) having the initial conditions

$$w^{*i}_j(0, a) = 0. \tag{36}$$

Let us suppose further that

$$v^{*i}_j(x) = w^{*i}_j(1, x). \tag{37}$$

Then the functions $v^{*i}_j(x)$ satisfy relations (14) and (15), where e is the origin of the coordinates. Moreover the following relations hold:

$$v^{*i}_j(x) x^j = x^i. \tag{38}$$

PROOF. In order to establish (14) we must solve system (35) for $a = e$. Obviously this solution is $w_j^{*i}(t) = \delta_j^i t$, i.e., $v_j^{*i}(e) = \delta_j^i$ (see (37)).

Relations (15) and (38) are proved by the same method, but in order to make this method clear we shall first take up the simpler case of (38).

Let

$$h^i(t) = w_j^{*i}(t, a)a^j - ta^i. \tag{39}$$

We shall show that $h^i(t) = 0$. Relation $h^i(1) = 0$ gives (38). First of all it is clear that

$$h^i(0) = 0. \tag{40}$$

We now calculate the derivative of the function $h^i(t)$. Making use of relations (35) and (33) we get

$$\frac{dh^i(t)}{dt} = (\delta_j^i + c_{\alpha\beta}^{*i} a^\alpha w_j^{*\beta}(t, a))a^j - a^i = c_{\alpha\beta}^{*i} a^\alpha w_j^{*\beta}(t, a)a^j$$
$$= c_{\alpha\beta}^{*i} a^\alpha (w_j^{*\beta}(t, a)a^j - ta^\beta).$$

Hence the function $h^i(t)$ satisfies the system of linear equations

$$\frac{dh^i}{dt} = c_{\alpha j}^{*i} a^\alpha h^j. \tag{41}$$

With the initial condition $h^i(0) = 0$ the system (41) has the obvious solution $h^i(t) = 0$, hence, because of the uniqueness of the solution of the system (41), we have $h^i(t) = 0$ (see (40)).

To prove relations (15) we let

$$h_{jk}^i(t) = \frac{\partial w_k^{*i}(t, a)}{\partial a^j} - \frac{\partial w_j^{*i}(t, a)}{\partial a^k} - c_{\alpha\beta}^{*i} w_j^{*\alpha}(t, a) w_k^{*\beta}(t, a) \tag{42}$$

and show that $h_{jk}^i(t) = 0$. Then the special case $h_{jk}^i(1) = 0$ gives us (15).

Since $w_j^{*i}(0, a) = 0$, it follows that $\partial w^{*i}(0, a)/\partial a^k = 0$ and therefore

$$h_{jk}^i(0) = 0. \tag{43}$$

We now calculate the derivative of the function $h_{jk}^i(t)$. Differentiating relations (35) we get

$$\frac{\partial^2 w_k^{*i}(t, a)}{\partial t \partial a^j} = c_{j\beta}^{*i} w_k^{*\beta}(t, a) + c_{\alpha\beta}^{*i} a^\alpha \frac{\partial w_k^{*\beta}(t, a)}{\partial a^j}. \tag{44}$$

Making use of (35) and (44) we get

$$\frac{dh_{jk}^i}{dt} = c_{j\beta}^{*i} w_k^{*\beta} + c_{\alpha\beta}^{*i} a^\alpha \frac{\partial w_k^{*\beta}}{\partial a^j} - c_{k\beta}^{*i} w_j^{*\beta} - c_{\alpha\beta}^{*i} a^\alpha \frac{\partial w_j^{*\beta}}{\partial a^k}$$
$$- c_{\alpha\beta}^{*i}(\delta_j^\alpha + c_{\gamma\beta}^{*\alpha} a^\gamma w_j^{*\beta})w_k^{*\beta} - c_{\alpha\beta}^{*i} w_j^{*\alpha}(\delta_k^\beta + c_{\gamma\delta}^{*\beta} a^\gamma w_k^{*\delta}).$$

Collecting similar terms in the last equation we get by means of (33) and (34)

$$\frac{d\overset{i}{h}_{jk}}{dt} = \overset{*i}{c}_{\alpha\beta}a^{\alpha}\left(\frac{\partial \overset{*\beta}{w_k}}{\partial a^j} - \frac{\partial \overset{*\beta}{w_j}}{\partial a^k} - \overset{*\beta}{c}_{\gamma\delta}\overset{*\gamma}{w_j}\overset{*\delta}{w_k}\right) = \overset{*i}{c}_{\alpha\beta}a^{\alpha}\overset{\beta}{h}_{jk}.$$

Hence the function $h^i_{jk}(t)$ is a solution of the system of equations

$$\frac{d\overset{i}{h}_{jk}}{dt} = \overset{*i}{c}_{\alpha\beta}a^{\alpha}\overset{\beta}{h}_{jk}, \tag{45}$$

having the initial conditions (43). With these initial conditions the system (45) has the obvious solution $h^i_{jk} = 0$, so that it follows from the uniqueness of its solution that $h^i_{jk}(t) = 0$. This proves Theorem 71.

This completes the second step of the construction of a local Lie group from its structural constants. We now state the whole construction in a final form.

THEOREM 72. *Let c^i_{jk} be constants satisfying relations* (11) *and* (12) *of* §48. *We consider the system of equations*

$$\frac{d\overset{i}{w}_j}{dt} = \overset{i}{\delta}_j + \overset{i}{c}_{\alpha\beta}a^{\alpha}\overset{\beta}{w}_j, \tag{46}$$

where a is a constant vector and w^i_j are unknown functions of the parameter t. We denote by $w^i_j(t, a)$ the solution of the system (46) *with the initial conditions*

$$\overset{i}{w}_j(0, a) = 0. \tag{47}$$

Let

$$\overset{i}{v}_j(x) = \overset{i}{w}_j(1, x). \tag{48}$$

Since the system (46) *is linear with constant coefficients, its solution is defined for an arbitrary vector a and for an arbitrary value of the parameter t. Therefore the functions $v^i_j(x)$ are defined for arbitrary values of the coordinates of the point x, i.e., over the whole Euclidean space. We consider, furthermore, the system of partial differential equations*

$$\overset{i}{v}_k(f)\frac{\partial f^k}{\partial x^j} = \overset{i}{v}_j(x). \tag{49}$$

The integrability conditions for this system of equations are satisfied, and since the matrix $\|v^i_j(x)\|$ becomes a unit matrix at the origin of coordinates e, there exists a sufficiently small neighborhood G of the origin e such that for $x \in G$, $y \in G$, there exists a solution $f(x, y)$ of the system (49) *which satisfies the initial condition*

$$f(e, y) = y. \tag{50}$$

We define the product of two points x and y in G by

$$xy = f(x, y). \tag{51}$$

By virtue of this law of multiplication G is a local Lie group taken in canonical coordinates of the first kind, and the structural constants of this group coincide with the preassigned numbers c^i_{jk}. If furthermore G^* is an arbitrary local Lie group, considered in canonical coordinates of the first kind, and having for structural constants the same numbers c^i_{jk}, then the function $f^*(x, y)$ which defines the law of multiplication in G^* coincides with the function $f(x, y)$ which we have defined above.

We have therefore shown the existence and the uniqueness of a local Lie group. It is worth noting that the function $f(x, y)$ which we have obtained above is an analytic function, because the systems of equations which we had to solve are analytic. Therefore *every local Lie group admits analytic coordinates.*

The proof of Theorem 72 follows directly from propositions A), B), C) and Theorems 70 and 71.

We now formulate the above result in terms of infinitesimal groups.

THEOREM 73. *Let R be an arbitrary infinitesimal group* (see Definition 46). *Then there exists a local Lie group G such that the infinitesimal group of the group G is isomorphic with the group R* (see Theorem 66). *Let G and G' be two local Lie groups, and R and R' their infinitesimal groups. Suppose there exists an isomorphic mapping g of the group R on the group R'. Then there exists one and only one locally isomorphic mapping h (up to an equivalence) of the local group G on the local Lie group G'* (see §34, K)) *which is such that the mapping of the group R on the group R' which corresponds to it* (see Theorem 68) *coincides with the given mapping g.*

PROOF. In order to construct the group G from its infinitesimal group R it is sufficient to take the group R in coordinate form. Since the structural constants of the group R satisfy relations (11) and (12) of §48, it follows from Theorem 72 that it is possible to construct the local Lie group G.

We select in the groups R and R' coordinate systems which correspond to each other under the mapping g. Then the structural constants of the groups R and R' will coincide.

Taking corresponding canonical coordinates of the first kind in the groups G and G' we obtain in them the functions $f(x, y)$ and $f'(x, y)$, which define the law of multiplication, and which coincide in case the structural constants of the groups coincide (see Theorem 72). In this way if we associate with each point $x \varepsilon G$ a point $x' \varepsilon G'$ whose coordinates are equal to the coordinates of the point x, we shall obtain the desired isomorphic mapping h. The uniqueness of the mapping h follows from the fact that every automorphism of the group G' can be written in canonical coordinates in the form of a linear transformation (see §42, B)). In this way to a non-identical automorphism of the group G corresponds a non-identical automorphism of the group R'. This completes the proof of Theorem 73.

Theorem 73 shows that the study of local Lie groups is completely reduced to the study of their infinitesimal groups.

It should be noted that the above method of constructing a Lie group from its infinitesmal group is primarily of theoretical interest. From a practical point of view it is more convenient to construct a Lie group from a given infinitesimal group from entirely different considerations and to make use of Theorem 73 only as a uniqueness theorem.

Example 66. We consider the structure of a two-dimensional Lie group. Let R be a 2-dimensional infinitesimal group and p and q two linearly independent vectors of R. Let $[p, q] = r$. It is not hard to verify that for any two vectors a and b of R we have $[a, b] = \alpha r$, where α is some number. We shall distinguish two cases: $r = 0$, and $r \neq 0$. If $r = 0$, then the commutator of any two vectors of R is equal to zero, and the group R is commutative. In case $r \neq 0$, there exists a vector t such that $[r, t] = r$. We take the vectors r and t as the basis of the space R. Then the structural constants have the values $c_{12}^1 = 1, c_{12}^2 = 0$. Hence there exists only two non-isomorphic two-dimensional infinitesimal groups.

If the group R is commutative, then the Lie group G which corresponds to it is also commutative.

If the group R is not commutative, then the corresponding group G can be defined by the relations

$$f^1 = x^1 + y^1 e^{-x^2}, \qquad f^2 = x^2 + y^2.$$

The set of all elements of the group G which have zero for their second coordinate forms a normal subgroup of the group G. The normal subgroup of the group R which corresponds to it is composed of all vectors of the form αr, where α is an arbitrary number.

52. The Construction of a Subgroup and of a Homomorphism

In the preceding section we have established the complete equivalence of the concepts of a local Lie group G and of its infinitesimal group R. We shall examine here this equivalence in greater detail by establishing a one-to-one correspondence between the subgroups, normal subgroups, and factor groups of the groups G and R. We have already arrived at the group R from the group G (see §49). Here we shall proceed in the opposite direction. It should be noted that all the considerations of the present section are of a purely local character.

Theorem 74. *Let G be a local Lie group, R its infinitesimal group, and S a subgroup of the group R. Then there exists, up to an equivalence, one and only one subgroup H of the group G* (see §23, I)), *which is such that the subgroup which corresponds to it in R is S. We shall say that the subgroups H and S correspond to each other, and write $H \rightleftarrows S$.*

Proof. Let r and s be the dimensions of the spaces R and S. We select in R a system of coordinates such that the vector a belongs to the subspace S if and only if its coordinates satisfy the relations

(1) $$a^{s+1} = 0, \cdots, a^r = 0,$$

while we introduce in G the corresponding canonical coordinates of the first kind. We shall keep these coordinates in R and G throughout the whole proof. If the subgroup H exists, it is defined in the coordinates chosen above by a system of linear equations (see §42, B)). Since the subgroup S must correspond to the subgroup H, it follows that H must be defined by the equations

$$x^{s+1} = 0, \quad \cdots, x^r = 0, \tag{2}$$

i.e. the point x belongs to the subgroup H if and only if its coordinates satisfy relations (2). Hence the uniqueness of the subgroup H is proved. We shall now prove its existence.

We denote by H the set of all points of G whose coordinates satisfy conditions (2) and show that H is a subgroup of the group G. To do this it is sufficient to show that if $x \in H$, $y \in H$, then $xy \in H$ and $x^{-1} \in H$. The proof will consist in a direct calculation of the function $f(x, y)$ which defines the law of multiplication in G carried out in the coordinates selected above (see §48, (1)).

Let c^i_{jk} be the structural constants of the group G or, what is the same, of the group R. Since a subgroup is defined by relations (1), it follows that the structural constants satisfy the following relations

$$\text{if } i > s, j \leqq s, k \leqq s, \text{ then } c^i_{jk} = 0. \tag{3}$$

In order to avoid indicating each time what the possible values of a certain index may be, we agree to write a prime (′) after all indices which assume only the values $1, \cdots, s$ and a double prime (″) after indices which assume the values $s + 1, \cdots, r$. With this notation relation (3) can be written

$$c^{i''}_{j'k'} = 0. \tag{4}$$

In the same way if a point (or a vector) belongs to H (or to S) we shall prime the letter by which it is represented.

We shall now occupy ourselves with the solution of the system of equations (46) of §51 for $a = a' \in S$. To do this we divide this system into two independent systems

$$\frac{dw^i_{j'}}{dt} = \delta^i_{j'} + c^i_{\alpha'\beta} a^{\alpha'} w^\beta_{j'} \tag{5}$$

and

$$\frac{dw^i_{j''}}{dt} = \delta^i_{j''} + c^i_{\alpha'\beta} a^{\alpha'} w^\beta_{j''}. \tag{6}$$

In order to find the solution of the system (5) we first find the solution of the system

$$\frac{d\overset{*}{w}{}^{i'}_{j'}}{dt} = \delta^{i'}_{j'} + c^{i'}_{\alpha'\beta'} a^{\alpha'} \overset{*}{w}{}^{\beta'}_{j'}. \tag{7}$$

It can easily be seen that in view of (4) the system (5) is satisfied if we let

$$w_{j'}^{i'} = \overset{*}{w}{}_{j'}^{i'}, \tag{8}$$

$$w_{j'}^{i''} = 0. \tag{9}$$

Because of the uniqueness of the solution of the system (46) of §51 we obtain the result

$$w_{j'}^{i''}(t, a') = 0 \tag{10}$$

from which it follows that

$$v_{j'}^{i''}(x') = 0 \tag{11}$$

(see §51, (48)).

We note that the functions $v_{j'}^{i'}(x')$ which we have obtained from (8) are auxiliary functions of some Lie group whose infinitesimal group is the group S. In fact we have $v_{j'}^{i'}(x') = w_{j'}^{*i'}(1, x')$, where the functions $w_{j'}^{*i'}(t, a')$ are obtained by integrating the system (7), while the constants $c_{j'k}^{i'}$ which enter into this system are the structural constants of the group S.

We now proceed to the solution of the system (49) of §51. We are interested only in the function $f^i(x', y')$. In fact we want to show that $f^{i''}(x', y') = 0$, since this will show that $f(x', y') \in H$. Since for a fixed y' the function $f(x', y')$ depends only on the variables $x^{i'}$, $i' = i, \cdot \quad , s$, it is sufficient to solve the system

$$v_k^i(f) \frac{\partial f^k}{\partial x^{j'}} = v_{j'}^i(x'). \tag{12}$$

In order to solve this system, we first solve the system

$$v_{k'}^{i'}(f^*) \frac{\partial f^{*k'}}{\partial x^{j'}} = v_{j'}^{i'}(x'), \tag{13}$$

with the initial conditions $f^{*i'}(e, y') = y^{i'}$. The system (13) is solvable since the functions $v_{j'}^{i'}(z')$ are, as we have seen, auxiliary functions of some Lie group. It can now readily be seen that the system (12) is satisfied by $f^{i'}(x', y') = f^{*i'}(x', y')$, $f^{i''}(x', y') = 0$, in view of (11). Because of the uniqueness of the solution of the system (12) we get the sought-for result, $f^{i''}(x', y') = 0$. Hence $x'y' = f' \in H$.

In order to prove that $(x')^{-1} \subset H$, it is sufficient to point out that in canonical coordinates of the first kind the element x^{-1} has the coordinates $-x^i$, $i = 1, \cdots, r$. This fact follows readily from the consideration of one-parameter subgroups. Hence $(x')^{-1} = z' \in H$, and Theorem 74 is proved.

Before passing on to the discussion of normal subgroups, we introduce the important concept of the adjoint group, which will form the foundation for the proof of Theorem 75.

A) Let G be a local Lie group taken in canonical coordinates of the first

kind. To every element $x \varepsilon G$ corresponds an inner automorphism a_x of the group G, i.e., if $z \varepsilon G$, then

$$a_x(z) = xzx^{-1}. \tag{14}$$

Because the coordinates are canonical, relation (14) can be written in coordinate form as follows.

$$a_x^i(z) = p_j^i(x)z^j \tag{15}$$

(see §42, B)).

It is not hard to see that $p_j^i(xy) = p_k^i(x)p_j^k(y)$. Hence we have a homomorphic mapping g of the group G on the Lie group P of matrices. To every element $x \varepsilon G$ corresponds a matrix $\|p_j^i(x)\| = g(x)$. The group P of matrices is called the *adjoint group* of the group G. The mapping g is now a homomorphic mapping of the group G on its adjoint group P, in which the kernel of the homomorphism g can easily be seen to be the center of the group G. The group P of matrices can also be thought of as a group of automorphisms of the infinitesimal group R of the Lie group G.

In order to calculate the functions $p_j^i(x)$ directly from the structural constants c_{jk}^i we replace x by ta, where ta represents a point whose coordinates are ta^i, a being a constant vector and t a parameter. Then the following relations hold:

$$\frac{dp_j^i(ta)}{dt} = c_{\alpha\beta}^i a^\alpha p_j^\beta(ta). \tag{16}$$

In other words, if we take into consideration the obvious initial conditions

$$p_j^i(0a) = \delta_j^i \tag{17}$$

we can determine the functions $p_j^i(x)$ by integrating the system (16).

To prove relations (16) we shall look for the functions $p_j^i(x)$ over a certain one-parameter subgroup $x(t)$ having the direction vector a. Because the coordinates are canonical, it follows that $x^i(t) = ta^i$. Furthermore we have

$$a_x(z) = xzx^{-1}z^{-1}z = q(x, z)z.$$

The last relation can be written in coordinate form as follows:

$$a_x^i(z) = z^i + c_{\alpha\beta}^i ta^\alpha z^\beta + \epsilon_1^i, \tag{18}$$

where ϵ_1^i is of the third order of magnitude with respect to t and with respect to the coordinates of the element z (see §48, (4), (8)). Comparing relations (15) and (18) we get

$$p_j^i(ta) = \delta_j^i + e_{\alpha j}^i ta^\alpha + \epsilon_j^i(t), \tag{19}$$

where $\epsilon_j^i(t)$ is of the second order of magnitude with respect to t. Since $x(t)$ is a one-parameter group we have

(20) $$\|p_j^i((t+\delta t)a)\| \cdot \|p_j^i(ta)\|^{-1} = \|p_j^i(\delta ta)\|.$$

It follows from (19) and (20) that

$$p_j^i((t+\delta t)a) - p_j^i(ta) = c_{\alpha\beta}^i \delta t a^\alpha p_j^\beta(ta) + \epsilon_\beta^i(\delta t) p_j^\beta(ta),$$

but the last relation implies (16).

B) We shall point out here one conclusion from relation (16), which however will not be used by us. It follows from A) that there exists a homomorphic mapping g of the group G on its adjoint group P. Since P can be regarded as a group of linear transformations of the space R, the elements of the infinitesimal group T of the Lie group P can be regarded as linear transformations of the space R (see Example 63). To the homomorphism g corresponds the homomorphism h of the infinitesimal group R on the infinitestimal group T (see Theorem 68). In this way to every element $a \varepsilon R$ corresponds a linear mapping $f_a = h(a)$ of the space R into itself. It follows from (16) that the mapping f_a is defined by the relation

(21) $$f_a(u) = [a, u],$$

where $u \varepsilon R$. The set of all mappings of the form (21) forms an infinitestimal group T of mappings of a vector space into itself. The infinitesimal group T is called the *infinitesimal adjoint group* of the group R or of the group G.

THEOREM 75. *Let G be a local Lie group, H a subgroup of G, R the infinitesimal group of G, and S the subgroup of the group R which corresponds to the subgroup H, $H \rightarrow S$* (see Theorem 67). *If S is a normal subgroup of the group R, then H is a normal subgroup of the group G. If S is a central normal subgroup of the group R, then H is a central normal subgroup of the group G.*

PROOF. Let r and s be the dimensions of the groups G and H. We introduce in G canonical coordinates such that H will be defined by the relations

(22) $$x^{s+1} = 0, \cdots, x^r = 0.$$

Then the subgroup S will be defined in corresponding coordinates in R by the relations

(23) $$a^{s+1} = 0, \cdots, a^r = 0.$$

Just as in Theorem 74 we shall mark with a prime (′) the indices which assume the values $1, \cdots, s$ and with a double prime (″) the indices which assume the values $s+1, \cdots, r$. The elements which belong to H will also be marked with a prime.

To prove the theorem we have to clear up the question of the dependence of the elements of the group H on the inner automorphisms of the group G. To do this it is sufficient to calculate the matrix $\|p_j^i(x)\|$, using the method indicated in A).

Because of the special choice of coordinates in G and the fact that S is a

normal subgroup of the group R, the structural constants c_{jk}^{i} satisfy the relations

(24) $$c_{jk'}^{i''} = 0.$$

We integrate the system (16) by splitting it up into two independent systems:

(25) $$\frac{dp_{j'}^{i}(ta)}{dt} = c_{\alpha\beta}^{i} a^{\alpha} p_{j'}^{\beta}(ta),$$

(26) $$\frac{dp_{j''}^{i}(ta)}{dt} = c_{\alpha\beta}^{i} a^{\alpha} p_{j''}^{\beta}(ta).$$

In order to integrate the system (25) we first solve the system

(27) $$\frac{dp_{j'}^{*i'}(ta)}{dt} = c_{\alpha\beta'}^{i'} a^{\alpha} p_{j'}^{*\beta'}(ta).$$

It can readily be seen that in view of (24) the system (25) is satisfied for $p_{j'}^{i'}(ta) = p_{j'}^{*i'}(ta)$, and $p_{j'}^{i''}(ta) = 0$. In this way we get the result

(28) $$p_{j'}^{i''}(x) = 0.$$

In case S is a central normal subgroup we have $c_{jk'}^{i} = 0$ instead of (24). In this case the system (25) has the solution $p_{j'}^{i}(ta) = \delta_{j'}^{i}$, and hence

(29) $$p_{j'}^{i}(x) = \delta_{j'}^{i}.$$

In follows from (28) that $a_x(z') \varepsilon H$ (see (14) and (15)), i.e., H is a normal subgroup, while (29) shows that $a_x(z') = z'$ (see (14) and (15)), i.e., H is a central normal subgroup. This proves Theorem 75.

We now pass to the consideration of homomorphisms.

THEOREM 76. *Let G and G' be two local Lie groups, R and R' their infinitesimal groups, and let h be a homomorphic mapping of the group R on the group R'. Then there exists, up to an equivalence, one and only one locally homomorphic mapping f of the group G on the group G'* (see §23, K)) *such that the homomorphic mapping of the group R on the group R' which corresponds to it is the given mapping h* (see Theorem 68). *We shall say that the mappings f and h correspond to each other, and write $f \rightleftarrows h$.*

PROOF. Let S be the kernel of the homomorphism h. By Theorems 74 and 75 to the normal subgroup S of the group R corresponds the normal subgroup N of the group G, $N \rightleftarrows S$. Let $G^* = G/N$, and denote by f^* the natural homomorphic mapping of the group G on G^*, by R^* the infinitesimal group of the group G^*, and by h^* that homomorphism of the group R on the group R^* which corresponds to the homomorphism f^* (see Theorem 68). Then S is the kernel of the homomorphism h^*, since the kernel of the homomorphism f^* is N, and $N \rightleftarrows S$ (see Theorem 74).

Given an element $a^* \varepsilon R^*$ there exists a coset A of the subgroup S in the group R which goes into the element a^* under the homomorphism h^*, while under the homomorphism h the coset A goes into some element $a' \varepsilon R'$. Let $a' = h'(a^*)$. It is not hard to see that h' is an isomorphic mapping of the group R^* on the group R' for which the following condition is satisfied:

$$h(a) = h'(h^*(a)), \tag{30}$$

where a is an arbitrary element of R. By Theorem 73 there exists a uniquely defined isomorphic mapping f' of the group G^* on G' such that the mapping of the group R^* on the group R' which corresponds to it is h', $f' \rightarrow h'$. Let

$$f(x) = f'(f^*(x)). \tag{31}$$

Since $f^* \rightarrow h^*$ and $f' \rightarrow h'$, it follows from (30) and (31) that

$$f \rightarrow h \tag{32}$$

(see §49, E)).

If there exist two distinct homomorphisms f and f'' which satisfy (32), then, since the kernels of the homomorphisms f and f'' coincide, we would have a non-identical automorphism of the group G' such that the automorphism of the group R' which corresponds to it would be identical; but this is impossible in view of Theorem 73. Hence Theorem 74 is proved.

The following examples show that the considerations of the present section are really of a purely local character.

Example 67. Let G^2 be a two-dimensional toroidal group. Every element x of the group G^2 is defined by a pair of real numbers x^1, x^2 which are defined up to an additive integer. The *product* of two element $xy = f$ is defined by the relations $f^1 = x^1 + y^1, f^2 = x^2 + y^2$, where these equations are taken modulo 1. G^2 is a Lie group defined in the large, whose infinitesimal group we shall denote by R^2. We consider in G^2 a local one-parameter subgroup $x(t)$ defined by the relations $x^1(t) = a^1t$, $x^2(t) = a^2t$, where the ratio a^1/a^2 is irrational. To the local subgroup $\{x(t)\} = H$ corresponds a subgroup S of the infinitesimal group R^2. We shall show that no entire subgroup of G^2 corresponds to the subgroup S. Suppose such a subgroup H^* exists. Since the subgroup H^* is uniquely defined in the neighborhood of the identity by the subgroup S, it follows that the subgroups H^* and H must coincide there. We can conclude from the fact that H^* is an entire group that the group H^* must contain all the elements $x(t)$, $x^1(t) = a^1t$, $x^2(t) = a^2t$, for arbitrary t. Since the ratio a^1/a^2 is irrational, it follows readily that the group H^* is a set which is everywhere dense in G^2, and since H^* must be one-dimensional and closed in G^2 we have arrived at a contradiction.

It should be noted that the group G^2 is not simply connected, and if we had made all our constructions for the universal covering group of G^2 (see Definition 44), all would have been well. In the following example we shall show that in the case of a simply connected Lie group there also exists no one-to-one corre-

spondence between an entire subgroup of a Lie group and its infinitesimal group.

EXAMPLE 68. Let G be the group of all rotations of the four-dimensional Euclidean space E around the point 0, or what is the same, let G be the group of all orthogonal matrices of order four and determinant unity. If $u \varepsilon E$, then the rotation $\varphi \varepsilon G$ transforms the point u in the point $\varphi(u) = v \varepsilon E$. We consider the totality of all such rotations φ, which are defined by the relations

$$v^1 = \cos(s^1)u^1 + \sin(s^1)u^2, \qquad v^2 = -\sin(s^1)u^1 + \cos(s^1)u^2,$$
$$v^3 = \cos(s^2)u^3 + \sin(s^2)u^4, \qquad v^4 = -\sin(s^2)u^3 + \cos(s^2)u^4.$$

It is not hard to see that the above set of rotations with arbitrary s^1 and s^2 forms a two-dimensional subgroup G^2 of the group G, where G^2 is a toroidal group (see Example 67). In this way the group G^2 contains the same difficulties which were pointed out in Example 67. It is true that the group G is not simply connected, but the fundamental group of the manifold G is of the second order, and therefore the use of a universal covering group will not help matters.

In what follows we shall show that the situation is more favorable for normal subgroups.

53. Complex Lie Groups. Classification

It follows from Theorems 72 and 49 that analytic coordinates can be introduced uniquely, up to an analytic transformation, into every Lie group G. So far we have always supposed that the coordinates of the elements of the group G are real numbers. However, since the functions which define the law of multiplication (see §48, (1)) may be chosen to be analytic, the formulas which define the law of multiplication in coordinate form preserve their meaning for complex values of the coordinates In this way a local Lie group may be enlarged by adding to it elements with complex coordinates. In the set $\tilde{G}$ of complex elements thus obtained the same law of multiplication holds as in G and all the fundamental conditions are fulfilled in it. Obviously $\tilde{G}$ forms a local Lie group in the usual sense, since ordinary real coordinates may be introduced in $\tilde{G}$ by defining them as the real and imaginary parts of the former complex coordinates. We shall call $\tilde{G}$ a *complex Lie group*, or the *complex form* of the real Lie group G. Because of the uniqueness (up to an analytic transformation) of the choice of analytic coordinates in the group G, the group $\tilde{G}$ is determined uniquely by the group G; this determination is, of course, in a local sense only, but we do not consider any other aspects here.

The concept of a complex local Lie group may be introduced independently without reference to a real Lie group. In order to do this it is sufficient to note that relations (1) of §48 are analytic, and that the parameters which appear in these relations assume complex values. In doing this it may happen of course that a complex Lie group is not generated by any real Lie group. All the relations and definitions of the preceding sections are automatically extended to complex Lie groups. The concepts of structural constants and infini-

tesimal groups are introduced; only all this is done in the complex rather than the real domain. In particular, a complete correspondence is established between complex local Lie groups and their infinitesimal groups.

The meaning of this construction becomes clear when we consider that in the study of infinitesimal groups it is necessary to solve algebraic equations and therefore the introduction of complex numbers is quite natural. It is possible of course to avoid complex numbers by a roundabout way, but the introduction of a complex group seems more logical.

While a real group always has one and only one complex form, a complex group may have no real form at all, or have several real forms. In this way in order to apply results obtained for complex groups to real groups we have always to solve the additional question as to what real forms belong to a given complex group. This question becomes particularly acute in the classification of groups. Suppose that we have achieved a classification of a certain type of complex groups. In order to infer from this a classification of real groups of corresponding type, it is necessary to find all the real forms of each of these complex groups. This determination, however, is far from simple.

We now pass to the isolation of some important types of groups. We shall do this in terms of infinitesimal groups, recalling that there exists a complete correspondence between them and the local Lie groups.

A) A complex or real infinitesimal group R is called *commutative* if for $a \in R$, $b \in R$ we always have $[a, b] = 0$ (see Definition 46).

B) Let R be a complex or real infinitesimal group. We define by R_1 the minimal linear subspace (respectively complex or real) of the vector space R which contains all the elements of the form

$$(1) \qquad [a, b],$$

where $a \in R$, $b \in R$. R_1 is called the *commutator* of the group R, and is a normal subgroup of R. The factor group R/R_1 is commutative, and the normal subgroup R_1 can be characterized as the minimal normal subgroup having this property, i.e., if S is a normal subgroup of the group R such that R/S is commutative, then $R_1 \subset S$. In other words; we simply carry over the concept of a commutator subgroup from abstract groups to Lie groups.

In order to prove that the commutator subgroup R_1 is a normal subgroup it is sufficient to note that the commutator of an arbitrary vector $c \in R$ and a vector of the form (1) is also a vector of the form (1), since $[c, [a, b]] = [c, d]$, where $d = [a, b]$. The commutativity of the group R/R_1 follows directly from the definition of a factor group (see §49, B)). We shall now prove the minimum property. If R/S is commutative, then for arbitrary $a \in R$ and $b \in R$ we have $[a, b] \in S$ (see §49, B)). Hence $R_1 \subset S$.

C) Let R_0 be a complex or real infinitesimal group. We construct the sequence of groups

$$(2) \qquad R_0, R_1, \cdots, R_i, \cdots$$

where R_{i+1} is defined as the commutator subgroup of the group R_i (see B)). Obviously, if two members of the sequence (2) are equal, then all the remaining terms coincide with them. Furthermore, if two members are not equal, then their dimensions differ at least by unity. Therefore, since the dimension of R_0 is finite, the series (2) must eventually become stationary. If this sequence becomes stationary beginning with the null subgroup (i.e., the subgroup of the group R_0 which contains only zero), then the group R_0 is called *solvable.* This definition is entirely analogous to the corresponding definition in the theory of abstract groups (see Definition 9). We shall call the sequence (2) the *series of commutator subgroups* of the group R_0.

D) A complex or real infinitesimal group R is called *semi-simple* if it contains no solvable normal subgroups distinct from zero.

We now pass to the proof of some elementary propositions about solvable and semi-simple infinitesimal groups.

We note first of all that a number of the propositions proved in the first chapter for abstract groups can easily be generalized to infinitesimal groups.

E) Let R be a complex or real infinitesimal group, and S and T two of its subgroups. We shall understand by the *intersection* of two subgroups S and T the intersection of the sets S and T, and by the *sum* or *product* of the groups S and T the set $S + T$ composed of all elements of the form $a + b$ where $a \varepsilon S$, $b \varepsilon T$. With this understanding all the propositions and definitions about abstract groups which were given in §5 are applicable to infinitesimal groups. We shall review here only the concept of direct product.

We shall say that the infinitesimal group R *decomposes into the direct sum,* or *into the direct product,* of its normal subgroups S and T, if the intersection $S \cap T$ contains only the zero, and if the sum $S + T$ is equal to R. It is clear that just as in abstract groups, the group R can be constructed, up to an isomorphism, from the groups S and T (see §5, F)).

F) In order that a complex or real infinitesimal group R be solvable, it is sufficient that R contain a sequence of subgroups

$$(3) \qquad R'_0 = R, R'_1, R'_2, \quad , R'_i, \quad , R'_n = \{0\}$$

such that R'_{i+1} is a normal subgroup of the group R'_i and that the factor group R'_i/R'_{i+1} is commutative for $i = 0, \cdots, n - 1$.

The proof of proposition F) is by induction on the number $n + 1$ of elements of the sequence (3). We denote by R_1 the commutator subgroup of the group R. Since R/R'_1 is commutative, $R_1 \subset R'_1$ (see B)). It follows from this that the proposition is true for $n = 1$. We denote by S'_i the intersection of $R_1 \cap R'_{i+1}$, $i = 0, 1, \cdots, n - 1$. It is not hard to see that the sequence $S'_0, S'_1, \cdots, S'_{n+1}$ possesses the same properties with respect to the group $R_1 = S'_0$ as the series (3), but the number of its members is one less than the number of terms in (3). Hence it follows from the hypothesis of the induction that R_1 is a solvable group, but from this follows the solvability of the group R in view of the definition of solvability (see C)).

G) If a complex or real infinitesimal group R is solvable, then its subgroups and factor groups are also solvable.

Let S be a subgroup of the group R and let

$$R_0 = R, R_1, \cdots, R_n = \{0\}$$

be the series of commutator subgroups of the group R (see C)). We denote by S_i' the intersection $S \cap R_i$. It is not hard to see then that the series of subgroups

$$S_0' = S, S_1', \cdots, S_n' = \{0\}$$

satisfies the condition of remark F) and therefore the subgroup S is solvable. Let R^* be a factor group of the group R. We denote by R_i' the image of the group R_i in the group R^*. It can readily be shown that the series of subgroups

$$R_0' = R^*, R_1', \cdots, R_n'$$

satisfies the conditions of remark F) and therefore the factor group R^* is solvable.

H) If R is a complex or real infinitesimal group and S a solvable normal subgroup such that R/S is solvable, then R is also a solvable group.

We denote by

$$R_0^*, R_1^*, \cdots, R_k^* = \{0\}$$

the series of commutator subgroups of the group R/S, by R_i' the inverse image of the group R_i^* in the group R, and by

$$R_k' = S, R_{k+1}', \cdots, R_n' = \{0\}$$

the series of commutator subgroups of the group S. Then the series

$$R_0' = R, R_1', \cdots, R_k' = S, R_{k+1}', \cdots, R_n' = \{0\}$$

can easily be seen to satisfy the conditions of remark F), and therefore R is a solvable group.

THEOREM 77. *Let R be a complex or real infinitesimal group. Then there exists in R a maximal solvable normal subgroup S, i.e., a solvable normal subgroup S which has the property that every other solvable normal subgroup S′ of the group R is contained in S. Furthermore S may be characterized as that solvable normal subgroup of the group R which renders the factor group R/S semi-simple.*

PROOF. Let S be a solvable normal subgroup of the group R which is not contained in any other of its solvable normal subgroups. We shall show that it has the property of being a maximal solvable subgroup as stated in the theorem. Let S' be an arbitrary solvable normal subgroup of the group R, and let $S'' = S + S'$ (see E)). Then S'' is a normal subgroup of the group R. We shall show that the group S'' is solvable. We denote by D the intersection $S' \cap S$. By Theorem 2 (see E)), S''/S is isomorphic with S'/D. The last

group is solvable in view of proposition G). Hence it follows from H) that the group S'' is also solvable. If now S' is not contained in S, then S'' is a solvable normal subgroup which contains S and which is greater than S, which contradicts the assumption. Therefore $S' \subset S$.

We shall now show that R/S is a semi-simple group. Let us suppose the contrary to be true. Then there exists a solvable normal subgroup T^* of the group R/S which is distinct from zero. We denote by T the complete inverse image of the group T^* in the group R. Then the factor group T/S is isomorphic with T^* and therefore by H), T is a solvable normal subgroup of the group R. But if T^* is a non-zero normal subgroup of the group R/S, then T is greater than S, which contradicts the definition of the group S.

Let us now suppose that S' is a solvable normal subgroup of the group R which has the property that R/S' is a semi-simple group. We then show that $S' = S$. In fact, suppose $S' \neq S$. Then S' is a proper part of S and therefore the factor group R/S' contains a non-zero solvable normal subgroup S/S' (see G)). This proves Theorem 77.

All the above propositions are simple repetitions of corresponding theorems in the theory of abstract groups. Theorem 77 shows that in a certain weak sense the study of general infinitesimal groups can be reduced to the study of semi-simple and solvable groups. There is, however, a way of strengthening Theorem 77, although only for Lie groups. We give here this stronger theorem without proof, since the proof is too complicated to be given here (see [18] and [36]).

THEOREM 78. *Let R be an arbitrary complex infinitesimal group and S its maximal solvable normal subgroup. Then R contains a semi-simple subgroup T which is such that*

$$S + T = R, \qquad S \cap T = \{0\}$$

(see E)). *In this way R is, so to speak, decomposed into the direct sum of the normal subgroup S and the subgroup T. A true decomposition into a direct sum would have been achieved if the subgroup T were a normal subgroup.*

Theorem 78 hows that the knowledge of solvable and semi-simple groups is really quite important for the study of general groups.

We shall now establish some connections between real infinitesimal groups and their complex forms.

I) Let R be a real infinitesimal group and $\tilde{R}$ its complex form. Then $R \subset \tilde{R}$, and every vector c of $\tilde{R}$ can be represented uniquely in the form $c = a + bi$, where a and b are vectors of R, and $i = \sqrt{-1}$. In this way it is possible to introduce the concept of the complex conjugate of an element of the group $\tilde{R}$: the two elements $c = a + bi$ and $\bar{c} = a - bi$ will be called *complex conjugates* of each other. Furthermore, if M is a set of elements of R, we shall denote by $\overline{M}$ the set of all elements which are complex conjugates of the elements of the set M, and we shall say that the sets M and $\overline{M}$ are complex conjugates of each other. It is not hard to see that if S is a subgroup or a normal subgroup

of the group $\tilde{R}$, then $\bar{S}$ is correspondingly a subgroup or a normal subgroup of the group $\tilde{R}$.

J) Let R be a real infinitesimal group and $\tilde{R}$ its complex form. Then the groups R and $\tilde{R}$ are either both solvable or both insolvable.

We denote by

$$(4) \qquad R_0 = R, R_1, \cdots, R_i, \cdots$$

the series of commutator subgroups of the group R (see C)) and by $\tilde{R}_i$ the totality of all vectors of the group $\tilde{R}$ which can be represented in the form $a + bi$, where $a \in R_i$, $b \in R_i$. It is not hard to see that the sequence

$$(5) \qquad \tilde{R}_0 = \tilde{R}, \tilde{R}_1, \cdots, \tilde{R}_i, \cdots$$

forms the series of commutator subgroups of the group $\tilde{R}$. Proposition J) follows directly from the connection between the series (4) and (5).

K) Let R be a real infinitesimal group and $\tilde{R}$ its complex form. We denote by S the maximal solvable normal subgroup of the group R, and by $\tilde{S}$ its complex form. Then $\tilde{S}$ is the maximal solvable normal subgroup of the group $\tilde{R}$. We see in this way that the groups R and $\tilde{R}$ are either both semi-simple, or else neither of them is semi-simple.

In order to prove K) we denote by T the maximal normal subgroup of the group $\tilde{R}$ (see Theorem 77). It follows from I) that $\bar{T}$ is also a solvable normal subgroup of the group $\tilde{R}$ and therefore $\bar{T} \subset T$. Hence

$$(6) \qquad T = \bar{T}.$$

We denote now by U the set of all *real* vectors of T, i.e., the set of vectors c such that $\bar{c} = c$. If $a + bi \in T$ where a and b are real vectors, then it follows from (6) that $a \in T$ and $b \in T$, i.e., $a \in U$ and $b \in U$. Hence T coincides with the complex form of the group U, $T = \tilde{U}$, and it follows from J) that U is a solvable normal subgroup of the group R. Hence

$$(7) \qquad U \subset S.$$

On the other hand $\tilde{S}$ is a solvable normal subgroup of the group $\tilde{R}$ and therefore

$$(8) \qquad \tilde{S} \subset T = \tilde{U}.$$

It follows from relations (7) and (8) that $\tilde{U} = \tilde{S} = T$.

L) A complex or real infinitesimal group R is called *simple* if it has no normal subgroups other than the zero and the whole group R.

It should be noted that there exists one simple group which is not semi-simple. This is the one-dimensional infinitesimal group. Obviously it is simple, but it is not semi-simple because it is a solvable group. All other simple groups can readily be seen to be semi-simple also.

It should also be noted that if a real group is simple its complex form is not necessarily simple (see Example 72).

Our further investigations into infinitesimal groups have to do with their classification. Solvable groups still remain unclassified, but we can give a complete classification of semi-simple groups. This classification is effected by means of a very complicated set-up, which makes it impossible to give here complete proofs of all results. We therefore confine ourselves to a mere exposition of the results.

The following theorem reduces the classification of semi-simple groups to that of simple groups.

THEOREM 79. *If R is a complex or real semi-simple group, then it is decomposable into the direct product of simple non-commutative groups.*

This theorem is given here without proof (see [5]).

In order to present more clearly the results on the classification of semi-simple groups I state here, also without proof, the two following theorems of Weyl (see [35]).

THEOREM 80. *If G is a real compact semi-simple Lie group then every group G' which is locally isomorphic with the group G is also compact.*

Hence the property of compactness is a local property for semi-simple Lie groups and therefore depends only on the infinitesimal group R of the group G. Therefore we shall call the infinitesimal group R itself *compact* in this case.

THEOREM 81. *Every complex semi-simple infinitesimal group $\tilde{R}$ has a real compact form R* (see Theorem 80), *and this form is unique up to an isomorphism.*

The methods used in the classification of semi-simple infinitesimal groups allow us in the first place to give a classification of complex groups. Theorem 81 shows, however, that there exists a one-to-one correspondence between complex semi-simple groups and their compact real forms (see Theorem 80). In this way the classification of complex semi-simple groups gives automatically the classification of compact real semi-simple groups (see [19]). We also note that if a simple real group is compact, then its complex form is simple. In this way it follows from Theorem 81 that in order to give a complete classification of semi-simple complex groups, it is sufficient to give a complete classification of compact simple Lie groups up to local isomorphism. This classification is given by the following theorem, which like the preceding one, is given without proof (see [5]).

THEOREM 82. *Compact non-commutative simple Lie groups can be classified, up to local isomorphism, as follows. There are five isolated groups, whose dimensions are* 14, 52, 78, 133, *and* 248. (We cannot enter into a detailed consideration of these groups here.)

Besides the above five groups, there are four infinite series of groups

$$A_n, B_n, C_n \quad (n = 1, 2, \cdots) \qquad \text{and} \qquad D_n \quad (n = 3, 4, \cdots)$$
$$A_1 = B_1 = C_1, \qquad B_2 = C_2, \qquad A_3 = D_3.$$

The group A_n is composed of all unitary unimodular matrices of order $n + 1$, i.e., the elements $a \in A_n$ are the matrices $a = \|a_{ij}\|$ whose elements are complex numbers which satisfy the relations

$$\sum_{k=1}^{n+1} a_{ik}\bar{a}_{jk} = \delta_{ij},$$

and the determinant of the matrix $\|a_{ij}\|$ is equal to unity.

The group B_n is composed of all orthogonal matrices of order $2n + 1$ having a positive determinant, i.e., the elements $b \in B_n$ are the matrices $b = \|b_{ij}\|$ whose elements are real numbers satisfying the relations

$$\sum_{k=1}^{2n+1} b_{ik}b_{jk} = \delta_{ij},$$

and the determinant of the matrix $\|b_{ij}\|$ is equal to unity.

The group C_n is composed of all unitary matrices of order $2n$ which leave invariant the bilinear form

$$\sum_{i=1}^{2n}\sum_{j=1}^{2n} f_{ij}x_iy_j$$

whose coefficients f_{ij} have the following values:

$$f_{12} = -f_{21} = 1, f_{34} = -f_{43} = 1, \cdots, f_{2n-1,2n} = -f_{2n,2n-1} = 1,$$

while all the other f_{ij} are equal to zero. Hence the elements $c \in C_n$ are the matrices $c = \|c_{ij}\|$ whose elements are complex numbers which satisfy the relations

$$\sum_{k=1}^{2n} c_{ik}\bar{c}_{jk} = \delta_{ij}, \qquad \sum_{i=1}^{2n}\sum_{j=1}^{2n} f_{ij}c_{ik}c_{jl} = f_{kl},$$

and the determinant of the matrix $\|c_{ij}\|$ is equal to unity.

The group D_n is composed of all orthogonal matrices of order $2n$ with positive determinants, so that the elements $d \in D_n$ are the matrices $d = \|d_{ij}\|$ whose elements are real numbers satisfying the relations

$$\sum_{k=1}^{2n} d_{ik}d_{jk} = \delta_{ij},$$

and the determinant of the matrix $\|d_{ij}\|$ is equal to unity.

The classification of complex semi-simple groups was originally given by Killing, but his proofs were incomplete. They were corrected by Cartan (see [5]), and later van der Waerden (see [34]) gave, on the basis of results of Weyl (see [35]), a new, more geometrical, and more elegant proof.

We note here that the groups A_n and C_n are simply connected, while the groups B_n and D_n have a fundamental group of the second order (see §46, G) and Definition 42).

EXAMPLE 69. Let K be the quaternion field (see §37, A)). We denote by G the set of all quaternions whose norm is equal to unity. The set G can readily be seen to form a group under multiplication. Since G is a sphere in the space K, the space G is the three dimensional sphere, and is therefore simply connected. The center of the group G is composed, as can readily be seen, of the two quaternions $+1$ and -1; we designate the center by Z. In this way every group which is locally isomorphic with the group G is isomorphic either with the group G itself or with the factor group G/Z (see Definition 44).

Let R be the three dimensional subspace of the space K which is composed of all quaternions of the form $ai + bj + ck$. It can easily be seen that if $x \varepsilon R$ and $g \varepsilon G$, then $gxg^{-1} \varepsilon R$, and the norms of the quaternions x and gxg^{-1} are equal. In this way we associate with every quaterion $g \varepsilon G$ a certain rotation φ_g of the space R which transforms the vector x into the vector $\varphi_g(x) = gxg^{-1}$. It is not hard to see that it is possible in this way to get all the rotations of the space R, and that the rotation φ_g is the identity if and only if $g = \pm 1$, i.e., $g \varepsilon Z$. Hence the group of rotations of the three dimensional Euclidean space R is isomorphic with the group G/Z. The group G/Z enters into the classification in Theorem 82 as the group B_1.

EXAMPLE 70. Let K be the quaternion field and G the subgroup of quaternions of norm 1 (see Example 69). We associate with every pair of quaternions (g, h), $g \varepsilon G$, $h \varepsilon G$ the rotation φ_{gh} of the space K which transforms every vector $x \varepsilon K$ into the vector $\varphi_{gh}(x) = gxh^{-1}$. It is not hard to show that we get in this way all the rotations of the space K, and that the identical rotation φ_{gh} corresponds only to the pairs $(1, 1)$ and $(-1, -1)$. It follows from this that the group L of rotations of a four dimensional space K is locally isomorphic with the direct product of two groups isomorphic with the group G. Therefore, the group L decomposes locally into the direct product of two simple groups, and is itself only semi-simple, but not simple.

EXAMPLE 71. Let G be the group of quaternions of norm 1 (see Example 69). We denote by H the finite subgroup of order 8 of the group C which is composed of the units: ± 1, $\pm i$, $\pm j$, $\pm k$ (see §37, A)). The space G/H (see Definition 24) has for its fundamental group the group H (see Example 61). Hence G/H is a three dimensional manifold having a non-commutative fundamental group H.

EXAMPLE 72. Let R_n be the n-dimensional vector space. We denote by G_k^n the group of all linear transformations of the space R_n which leave invariant the non-degenerate quadratic form $\psi_k(x)$ which consists in its canonical form of $n - k$ positive and k negative squares. It is not hard to show that the group G_k^n is a real Lie group. It is obvious that the complex forms of all the groups G_k^n, $k = 0, 1, \cdots, n$, are isomorphic, since in complex form there is no distinction between the quadratic forms $\psi_k(x)$, $k = 0, 1, \cdots, n$. In their real forms the groups G_k^n and G_l^n are locally isomorphic only if $k + l = n$. In this case they are, of course, simply isomorphic. There is an obvious distinction between the groups G_0^n and G_1^n, since the group G_0^n is compact, while the group G_l^n is not.

It is worth noting that the group G_2^4 is simple in its real form, while the group G_0^4, as we have seen, (see Example 70) decomposes locally into a direct product. Hence the complex form of the real simple group G_2^4 is not simple, but only semi-simple.

We now consider the group G_1^3. We call a *ray* in the space R_3 the totality of all vectors of the form αx, where $x \varepsilon R_3$, and α is an arbitrary real number. The set of all rays of the space R_3 forms, as is well known, a *projective plane* P. The locus represented by the equation $\psi_1(x) = 0$ intersects the plane P in a real conic section V. In this way to every transformation of the group G corresponds a projective transformation of the plane P which leaves invariant the conic section V. Hence the group G_1^3 is locally isomorphic with the group of transformations of a projective plane P which have an invariant curve V. This last group is, as is well known, isomorphic with the group of rotations of a non-Euclidean plane, and also with the group of linear fractional transformations of a line.

We note that, up to a local isomorphism, there are only two three-dimensional simple Lie groups: The groups G_0^3 and G_1^3, the first of which is compact, while the second is not. The complex forms of G_0^3 and G_1^3 are locally isomorphic.

There are no two-dimensional simple Lie groups (see Example 67).

We also note the obvious fact that in the classification of Theorem 82, the group G_0^{2n+1} appears under the notation B_n, and the group G_0^{2n} as D_n.

54. The Construction of a Lie Group in the Large

We shall give here a construction of an entire Lie group from its structural constants. (An *entire* group is a group in the sense of Definition 1 as contrasted with a *local* group.) This construction depends on Theorem 78, which remains unproved in this book; but since Theorem 78 is of a purely local character this construction is not devoid of interest. We shall make constructions independent of Theorem 78 for groups having no center and for solvable groups.

We want to point out in advance that some of the details of the proofs which follow are not given with complete care and exactness. The trouble is that in a local group (see §23, D)) the operation of multiplication is not defined for every pair of elements, and therefore certain of the constructions given below have meaning not for the local group itself, but only for a sufficiently small part of it (see §23, G)). However, were we to attempt to define each time the proper portion of the group, and introduce a new notation for it, our text would be unnecessarily cluttered up with non-essential details. Therefore we take the liberty of talking about the local group itself, whereas, in some cases, we should be talking only about a certain part of this group.

A) If a local Lie group G' has no center, then a part of it can be contained in an entire Lie group G.

To prove this we consider the adjoint local Lie group P' of the group G' (see §52, A)). Since G' has no center, the mapping g of the group G' on the group P' is isomorphic on some part of the group G'. We denote by

$$(1) \qquad U_1, \quad \cdots, U_s, \cdots$$

a complete system of neighborhoods of the identity of the group P'. We denote furthermore by P the set of all finite products of matrices which belong to P'. The set P, as can easily be seen, forms an abstract group under multiplication. We introduce a topology into the group P by taking the system (1) for a complete system of neighborhoods of the identity. It is not hard to verify that the system (1) in the group P satisfies the conditions of Theorem 10, and therefore the group P is a topological group, and P' is contained in P as a neighborhood of the identity. Hence the local group P' is contained in the complete group P, and since G' and P' are locally isomorphic, Proposition A) is proved.

LEMMA. *Let G' be a local Lie group. Suppose G' contains a normal subgroup N' and a subgroup H' having the properties that the intersection $N' \cap H'$ contains only the identity, the product $N'H'$ coincides with G', and every element $g' \in G'$ can be represented uniquely in the form $g' = n'h'$, where $n' \in N'$, and $h' \in H'$. Let us also suppose that the local groups N' and H' can be included in the entire connected simply connected groups N and H, respectively* (see §46, F), G)). *We now form the topological product G of the spaces N and H, i.e., the set of all pairs (n, h), there $n \in N$, and $h \in H$* (see Definition 21). *We can define the law of multiplication in the group G in such a way that G becomes a topological group satisfying the following condition: if we associate with every element $g' = n'h' \in G'$ a pair of elements $(n', h') \in G$, we get a homeomorphic mapping χ of the local Lie group G' on some neighborhood of the identity of the group G, which is isomorphic on some part of the group G'. Hence G is an entire connected simply connected Lie group which contains a part of the group G' as a local group.*

PROOF. We consider the inner automorphism $\varphi'_{g'}$ of the group G' which is defined by the relations $\varphi'_{g'}(x) = g'xg'^{-1}$. Since N' is a normal subgroup of the group G', the automorphism $\varphi'_{g'}$ of the group G' is also an automorphism of the group N'. By Theorem 63 the automorphism $\varphi'_{g'}$ of the group N' can be extended uniquely to the automorphism $\varphi_{g'}$ of the entire group N. In this way to every element $h' \in H'$ corresponds a definite automorphism $\varphi_{h'}$ of the group N.

We denote by K' the set of all elements of the group H' to which corresponds the identical automorphism of the group N. Then the set L' of automorphisms of the type $\varphi_{h'}$ forms a local Lie group isomorphic with the factor group H'/K'. We denote by

$$(2) \qquad W_1, \cdots, W_n, \cdots$$

a complete system of neighborhoods of the identity of the group L', and by L the set of all finite products of automorphisms belonging to L'. Then L is an abstract group. We introduce a topology into L by taking the system (2) for the complete system of neighborhoods of the identity. It is not hard to check that the system (2) satisfies the conditions of Theorem 10, and therefore L is a group which contains L' as a local group.

From what we have already established, to every element $h' \varepsilon H'$ corresponds an automorphism $\varphi_{h'} \varepsilon L'$. Therefore we have a locally homomorphic mapping ψ' of the local group H' on the local group L'. By Theorem 63 the homomorphism ψ' can be extended in only one way into a homomorphism ψ of the entire group H on the entire group L. Therefore, to every element $h \varepsilon H$ corresponds a definite automorphism $\varphi_h = \psi(h)$ of the group N.

We now define the product of two pairs (n_1, h_1) and (n_2, h_2) of the set G as follows:

$$(n_1, h_1)(n_2, h_2) = (n_1\varphi_{h_1}(n_2), h_1h_2). \tag{3}$$

It is not hard to verify that by virtue of this law of multiplication the set G becomes a topological group.

We establish first of all the fact that G is an abstract group. We have

$$((n_1, h_1)(n_2, h_2))(n_3, h_3) = (n_1\varphi_{h_1}(n_2), h_1h_2)(n_3, h_3) = (n_1\varphi_{h_1}(n_2)\varphi_{h_1h_2}(n_3), h_1h_2h_3),$$

$$((n_1, h_1)(n_2, h_2)(n_3, h_3)) = (n_1h_1)(n_2\varphi_{h_2}(n_3), h_2h_3) = (n_1\varphi_{h_1}(n_2)\varphi_{h_1h_2}(n_3), h_1h_2h_3).$$

Hence the associative law is satisfied. The identity of the group G is the pair (e_n, e_h), where e_n is the unit of the group N, and e_h is the unit of the group H. The pair inverse to the pair (n, h) is $(\varphi_h^{-1}(n^{-1}), h^{-1})$. In fact (see (3)),

$$(n, h)(\varphi_h^{-1}(n^{-1}), h^{-1}) = (n\varphi_{hh^{-1}}(n^{-1}), hh^{-1}) = (e_n, e_h).$$

Hence in view of the multiplication law (3) the set G is an abstract group.

We shall show that the multiplication law (3) is continuous in the topological space G. To do this, we show first of all that the element $\varphi_h(n) \varepsilon N$ is a continuous function of the pair of elements $n \varepsilon N$ and $h \varepsilon H$. We denote by U and V such neighborhoods of the identities of the groups N' and H' that $VUV^{-1} \varepsilon N'$. Obviously for $n \varepsilon U$ and $h \varepsilon V$ the function $\varphi_h(n)$ is continuous, since $\varphi_h(n) = hnh^{-1}$. Let now $h \varepsilon V$, and let n be some fixed element of N. Since N is connected, $n = n_1, \cdots, n_k$, where $n_i \varepsilon U$, $i = 1, \cdots, k$ (see Theorem 15). Then

$$\varphi_h(n) = \varphi_h(n_1) \cdots \varphi_h(n_k).$$

Since we have already shown that $\varphi_k(n_i)$ is a continuous function of the element h, the last product is also a continuous function of the element h, since the multiplication law is continuous in the group N. Let $h \varepsilon V$, and let n be an arbitrary element of N. We can then write $n = n^*n'$, where n^* is fixed and n' is in U. We then have $\varphi_h(n) = \varphi_h(n^*)\varphi_h(n')$, and hence, from what we have already shown, the function $\varphi_h(n)$ is continuous for $h \varepsilon V$, and $n \varepsilon N$. Now let $h \varepsilon H$ and $n \varepsilon N$ be arbitrary variable elements; then we can write $h = h^*h'$, where h^* is fixed and $h' \varepsilon V$. We have $\varphi_h(n) = \varphi_{h^*}(\varphi_{h'}(n))$, where $\varphi_{h'}(n)$ has been shown to be a continuous function of the pair of elements h' and n. Furthermore $\varphi_h^*(\bar{n})$ is a continuous function of the element $\bar{n}$. Hence $\varphi_h(n)$ is a continuous functions of the pair of elements h and n.

It follows from the above that $n_1\varphi_{h_1}(n_2)$ is a continuous function of the elements n_1, h_1, and n_2. In the same way h_1h_2 is a continuous function of the elements h_1 and h_2. Therefore the law of multiplication (3) satisfies the conditions of continuity, and G is a topological group.

We now prove that the mapping χ is isomorphic on some part of the local group G'. Let $g_1 = n_1h_1$ and $g_2 = n_2h_2$ be two elements of the group G'. We then have $g_1g_2 = n_1h_1n_2h_2 = n_1h_1n_2h_1^{-1}h_1h_2 = (n_1\varphi_{h_1}(n_2))(h_1h_2)$. If we now multiply the corresponding pairs (n_1h_1) and (n_2h_2) in the group G, we get, in view of the multiplication law, $(n_1\varphi_{h_1}(n_2), h_1h_2)$. Obviously the mapping χ is homomorphic. This proves the lemma.

We note that the above lemma is true for real as well as for complex Lie groups (see §53).

We shall now apply this lemma to construct a solvable Lie group in the large.

THEOREM 83. *Let R be a solvable infinitesimal group* (see §53, C)). *Then there exists an entire connected simply connected Lie group G whose infinitesimal group is isomorphic with the given group R. The group G is homeomorphic to a Euclidean space, i.e., we can introduce in it cartesian coordinates $x^1, \cdots, x^r$. Moreover, there exists a set of cartesian coordinates having the following properties: 1) The multiplication law can be expressed in these coordinates by means of analytic functions defined in the whole group G, 2) If we denote by $g_i(t)$ a point whose coordinates are equal to zero with the exception of the i-th coordinate which is equal to t, then $g_i(t)$ is a one-parameter subgroup of the group G, and the coordinates of the point $g_1(t^1) \cdots g_r(t^r)$ are the numbers $t^1, \cdots, t^r$. We denote further by H_i the totality of all points of the form $g_1(t^1) \cdots g_i(t^i)$. Then H_i is a subgroup of the group G and a normal subgroup of the group H_{i+1}.*

PROOF. It is not hard to construct in a solvable infinitesimal group R an increasing sequence of subgroups

$$S_1, \cdots, S_r = R,$$

where the group S_i is of dimension i and is a normal subgroup of the group S_{i+1}. Let G' be a local Lie group having the infinitesimal group R (see Theorem 73). To the subgroup S_i corresponds a subgroup H_i' of G' (see Theorem 74). The group S_1 is a one-parameter group and the theorem is obvious for it. Suppose that the theorem has been proved for the group S_i. We then select in the group H_{i+1}' a local one-parameter subgroup $\{g_{i+1}'(t)\} = K_{i+1}'$ which is not in H_i'. Then $H_i'K_{i+1} = H_{i+1}$, and the intersection $H_i' \cap K_{i+1}$ contains only the identity, while H_i' is a normal subgroup of the group H_{i+1}' (see Theorem 75). We are therefore in a position to apply the lemma of the present section, since the group H_i has already been constructed in the large, while the group K_{i+1}' being a one-paraneter group, can be included in the entire group $K_{i+1}' = \{g_{i+1}(t)\}$. Hence we can represent every element of the entire group H_{i+1} in the form of a pair $(h_i, g_{i+1}(t))$, where $h_i \in H_i$. This completes the induction and proves Theorem 83. The analyticity of the law of multiplication follows directly from the

fact that every automorphism of the group H_i which is generated by the element $g_{i+1}(t)$ can be expressed in an analytic form.

We note that Theorem 83 is true for real as well as complex groups R.

THEOREM 84. *Let R be an arbitrary infinitesimal group. Then there exists an entire group G whose infinitesimal group is isomorphic with the given group R.* (Note that the proof of this theorem depends on Theorem 78, which was given above without proof.)

PROOF. Since Theorem 78 is formulated for complex groups, we first give a proof for a complex infinitesimal group $\tilde{R}$ which coincides with R if R is complex, and is the complex form of R if R is real.

Let $\tilde{G}'$ be a local Lie group having the infinitesimal group $\tilde{R}$ (see Theorem 73). By Theorem 78 the group $\tilde{R}$ contains a solvable normal subgroup $\tilde{S}$ and a semi-simple group $\tilde{T}$ such that the intersection $\tilde{S} \cap \tilde{T}$ contains only zero and the sum $\tilde{S} + \tilde{T}$ coincides with the whole group $\tilde{R}$. Let $\tilde{N}'$ and $\tilde{H}'$ be those subgroups of the group $\tilde{G}'$ which correspond to the subgroups $\tilde{S}$ and $\tilde{T}$ (see Theorem 74). Then $\tilde{N}'$ is a normal subgroup of the group $\tilde{G}'$, and the intersection $\tilde{N}' \cap \tilde{H}'$ contains only the identity, while the product $\tilde{N}'\tilde{H}'$ coincides with $\tilde{G}'$. The group $\tilde{N}'$, being solvable, may be included in the entire connected simply connected group $\tilde{N}$ (see Theorem 83). The group $\tilde{H}'$, being semi-simple, does not contain a center and therefore may be included in some entire connected group $\tilde{H}^*$ (see A)). Taking the universal covering group of this entire group (see §47) we get a simply connected group $\tilde{H}$, which contains the group $\tilde{H}'$ as a local group. We are therefore in a position to apply the lemma of the present section, i.e., to include the local Lie group $\tilde{G}'$ in the entire group $\tilde{G}$, where $\tilde{G}$ is simply connected, as can easily be seen.

We now pass to the consideration of the case in which $\tilde{R}$ is the complex form of a real group R. Then $\tilde{G}'$ is the complex form of that real local group G' whose infinitesimal group coincides with R. We associate with every element $x \in \tilde{G}'$ its complex conjugate element $\bar{x} = \psi'(x)$. It can readily be seen that the mapping ψ' is a local automorphism of the above constructed topological group $\tilde{G}$, and since the group $\tilde{G}$ is simply connected, this automorphism can be extended into an automorphism ψ of the entire group $\tilde{G}$ (see Theorem 63). We denote by G the set of all elements of the group $\tilde{G}$ which remain invariant under the automorphism ψ, i.e. such elements that $\psi(x) = x$. It is obvious that the set G is a subgroup of the topological group $\tilde{G}$. The set G can readily be seen to coincide with G' in the neighborhood $\tilde{G}'$, since in that neighborhood the real elements coincide with their conjugates. In this way a neighborhood of the identity of the group G coincides with the local group G'. Hence the local group G' is contained in the entire group G.

It is worth noting that we have now established in the group $\tilde{G}$ the concept of conjugate elements, i.e., we can suppose that the elements x and $\psi(x)$ are complex conjugates. We have therefore the right to assert that the group $\tilde{G}$ is the complex form of the real group G, while prior to this the concept of complex form had meaning only for local Lie groups, since it was defined in terms of

coordinates. It should be remembered, however, that the entire real group G thus obtained cannot be supposed to be given in advance. All we know is that G is a real Lie group having a given infinitesimal group R. The complex group $\tilde{G}$ is defined uniquely, since it is connected and simply connected, and therefore the group G is also uniquely defined. However, if we are given an entire real Lie group G, the question as to its complex form in the large is undetermined.

THEOREM 85. *Let G be an entire simply connected Lie group and let N' be a local normal subgroup of G. Then a certain part of the Lie group N' may be included in an entire normal subgroup N of the group G.* (It should be noted that the analogous theorem would not be true for a local subgroup H' of the group G which is not a normal subgroup (see Example 68)).

PROOF. Let G' be a small neighborhood of the identity of the group G. Then G' is a local Lie group, and N' is a normal subgroup. The factor group $G'/N' = K'$ (see §23, J)) is a local Lie group and therefore can be included in the entire connected simply connected Lie group K (see Theorem 84). The natural homomorphic mapping f' of the group G' on the group K' is a local homomorphism of the group G on the group K and, since G is simply connected, the homomorphism f' can be extended into a homomorphism f of the entire group G in the entire group K (see Theorem 63). We denote the kernel of the homomorphism f by N. It is not hard to see that N is an extension of a certain part of the local group N'.

I do not know whether Theorem 85 holds in case the group G is not simply connected, and whether the normal subgroup N obtained in this theorem is simply connected or not. The fact that the normal subgroup N is connected follows readily from the simple-connectedness of the group K.

EXAMPLE 73. The method used in the proof of the lemma given in this section is also useful for the construction of examples of Lie groups.

Let N be the r-dimensional Euclidean space, which we shall also consider as an additive vector group. Let H be the group of all rotations in the space N; with each element $x \varepsilon H$ is associated a rotation φ_x of the Euclidean space N. The rotation φ_x is an automorphism of the group N. We now define the group G as the set of all pairs of the form (n, h), where $n \varepsilon N$, and $h \varepsilon H$. The law of multiplication is defined by letting

$$(n_1, h_1)(n_2, h_2) = (n_1\varphi_{h_1}(n_2), h_1h_2).$$

It is not hard to show that G is a Lie group, N a normal subgroup, and H a subgroup.

Making use of this method we can include every Lie group N in some group G in such a way that every automorphism of the group N can be realized by means of some inner automorphism of the whole group G.

55. Compact Lie Groups

Compact Lie groups have a much simpler local structure than general Lie groups. This simplicity is explained by the possibility of invariant integration

over compact groups. It is true that invariant integration is possible over some non-compact Lie groups, but in this case the volume of the entire group is infinite, while it is finite for compact groups. Invariant integration can easily be established independently for Lie groups, but I shall refer here to the results of Chapter IV. We have established there invariant integration over a compact group, and have proved Theorem 23 on the basis of this integration. If we remain in the real domain, then Theorem 23 can be applied to Lie groups in the following form:

A) Let g be a representation of a compact Lie group G, i.e., we associate with every element $x \varepsilon G$ a square matrix $g(x) = \|g_{ij}(x)\|$ in such a way that the mapping g of the group G into the multiplicative groups of matrices is homomorphic. Then there exists a constant matrix m, not depending on x, such that all the matrices of the form $mg(x)m^{-1}$ are orthogonal.

This is the only result of Chapter 4 which we shall use here.

B) Let R be the infinitesimal group of the compact Lie group G. Then every normal subgroup S of the group R is also a *direct cofactor*, i.e., there exists for every normal subgroup S a normal subgroup T such that the intersection $S \cap T$ contains only zero and the sum $S + T$ coincides with R. It is important to note that every normal subgroup R' of the group R possesses this property, i.e., every normal subgroup S' of the group R' is also a direct cofactor of the group R'.

To prove this let us consider the complete adjoint group P of the group G (see §52, A)). The homomorphic mapping g of the group G on the group P gives a representation of the group G. By A) we can introduce in G a linear transformation of coordinates such that all the matrices $\|p_j^i(x)\| = g(x)$ become orthogonal. We select in R a corresponding set of coordinates and consider the matrices $\|p_j^i\|$ as linear transformations of the vector space R. Since S is a normal subgroup of the group R, the linear space S remains invariant under all the transformations of the matrices $\|p_j^i(x)\|$. Since these matrices are orthogonal, the linear subspace T, which is orthogonal to S, is also invariant under all the transformations of the matrices $\|p_j^i(x)\|$. We shall now suppose that the coordinates in R are selected in such a way that the first s axes lie in S and the remaining $r - s$ axes lie in T. With this choice of coordinates every matrix $\|p_j^i(x)\|$ decomposes into two square matrices of orders s and $r - s$. We can derive from this fact some conclusions about the behavior of structural constants by use of equations (16) of §52. Because the vector a is perfectly arbitrary, we can conclude that the constants c_{jk}^i are zero for $k > s$ and $i < s$, and this means that for $b \varepsilon T$ and an arbitrary vector $a \varepsilon R$ we have $[a, b] \varepsilon T$, i.e., T is a normal subgroup.

Now let R' be a normal subgroup of the group R, and S' a normal subgroup of the group R'. From what we have shown above R' is a direct cofactor of the group R, and therefore S' is a normal subgroup of the group R. In this way S' is a direct cofactor of the whole group R, i.e., there exists a normal subgroup T of the group R such that the intersection $S' \cap T$ contains only zero,

and the sum $S' + T$ coincides with R. If we denote by T' the intersection $T \cap R'$, then it can readily be seen that R' decomposes into the direct product of the groups S' and T'.

This proves proposition B).

THEOREM 86. *Let R be the infinitesimal group of a compact Lie group G. Then R decomposes into the direct product of a finite number of non-commutative simple groups $S_1, \cdots, S_k$ and its center S_0. This decomposition is unique, i.e. the subgroups*

$$S_0, S_1, \cdots, S_k \tag{1}$$

are uniquely defined.

PROOF. If the group R is not simple, then R is decomposable by B) into the direct product of two normal subgroups S and T. If these groups in turn are not simple, the process of decomposition is continued until we arrive at indecomposable factors. We denote the non-commutative factors by $S_1, \cdots, S_k$. The direct product of the one-dimensional commutative factors can easily be seen to form the center S_0 of the group R.

We now pass to the proof of the uniqueness of the above decomposition. Suppose that there exists still another decomposition

$$T_0, T_1, \cdots, T_l, \cdots. \tag{2}$$

We shall then show that there exists a one-to-one correspondence between the groups of the decompositions (1) and (2) such that the corresponding groups completely coincide, and therefore the decompositions (1) and (2) do not differ from each other.

First of all it is clear that $T_0 = S_0$, since each of these subgroups is the center of the group R.

Let $a \varepsilon R$. We then have

$$a = \varphi_0(a) + \varphi_1(a) + \cdots + \varphi_l(a), \tag{3}$$

where $\varphi_j(a) \varepsilon T_j$, $j = 0, 1, \cdots, l$. Let, furthermore, $b_i \varepsilon S_i$, $i \geqq 1$. Since the group S_i, $i \geqq 1$, is not commutative, and has no center, there exists an element $a \varepsilon R$ such that $[b_i, a] \neq 0$. It follows from this and from relation (3) that there exists a number j such that $c = [b_i, \varphi_i(a)] \neq 0$. But then the element c belongs to both S_i and T_j, so that the group S_i and T_j have an element in common which is distinct from zero. Since the intersection of two normal subgroups is also a normal subgroup, the intersection of the groups S_i and T_j is a normal subgroup of the group R. But the group S_i is simple; hence $S_i \subset T_j$. It follows from this that $j \neq 0$, since T_0 is the center. Furthermore, since T_j is a simple group, $S_i = T_j$. Hence we have shown that every normal subgroup S_i, $i \geqq 1$, coincides with one of the normal subgroups T_j, $j \geqq 1$. Obviously two distinct normal subgroups S_i and $S_{i'}$ cannot coincide with the same normal subgroup T_j. Therefore to every normal subgroup S_i corresponds a definite normal subgroup T_j which coincides with it. It is clear that this

correspondence exhausts all the normal subgroups T_j, for in the contrary case the direct product of all the normal subgroups (1) would not be equal to the group R. This proves Theorem 86.

We give here a simple consequence of proposition B) and Theorem 86.

C) A compact connected Lie group G is semi-simple if and only if its center is discrete (see §53, D)).

Let R be the infinitesimal group of the group G. From its definition the group G is semi-simple if and only if R is semi-simple. If G has a non-discrete center, then R has a center distinct from zero, and therefore R is not semi-simple. On the other hand, if R is not semi-simple then there exists a solvable normal subgroup S of the group R. By B) there exists a normal subgroup T of the group R such that R is the direct product of the groups S and T. Since S is solvable, the commutator subgroup S' of the group S is distinct from S, and hence S decomposes by B) into the direct product of the groups S' and S''. Since the factor group S/S' is commutative (see §53, B)), S'' is also commutative. Decomposing S', S'', and T further until we reach the simple factors, we arrive at a decomposition of the group R which contains a commutative factor arising from S''. This factor must belong to the center of the group R by Theorem 86. In this way the group R has a center S_0 which is distinct from zero.

We now denote by Z_0' the local subgroup of the group G which corresponds to the subgroup S_0 (see Theorem 74). Then Z_0' is a central local normal subgroup of the group G. We denote by Z_0 the set of all finite products of elements which belong to Z_0'. It is obvious that Z_0 is a central normal subgroup of the abstract group G. The closure $\overline{Z}_0$ of the set Z_0 in the space G is a central normal subgroup of the Lie group G (see §22, D)). Hence G has a non discrete center.

On the basis of the above results we can readily understand the structure of a compact Lie group in the large. It is true that in doing this we have had to make use of Weyl's theorem, which remains unproved in this book (see Theorem 80).

THEOREM 87. *Every connected compact Lie group can be obtained by the following method. Let*

$$H_1, \cdots, H_k \tag{4}$$

be a finite system of compact connected simply-connected non commutative simple Lie groups and let

$$K_1, \cdots, K_l \tag{5}$$

be a finite system of one-dimensional compact connected Lie groups. We form the direct product G^* of all the groups of the systems (4) *and* (5). *We then take a normal subgroup N of the group G^* and form the factor group $G^*/N = G$. The set of all compact groups G obtained in this way coincides with the set of all compact connected Lie groups. (We note the obvious fact that each one of the groups K_j*

is isomorphic with the factor group D/C, where D is the additive group of real numbers and C is the subgroup of integral numbers.)

Proof. Let G be an arbitrary compact connected Lie group, and let R be its infinitesimal group. By Theorem 86 the group R decomposes into the direct product of simple normal subgroups $S_1, \cdots, S_k$ and its center S_0. Let H'_i be the local subgroup of the group G which corresponds to the subgroup S_i (see Theorem 74). We denote by H_0 the set of all finite products of elements belonging to H'_0. Then H_0 is obviously a central normal subgroup of the abstract group G. We shall show that H_0 is a closed set in the space G, and therefore is a central normal subgroup of the topological group G. We consider the closure $\overline{H}_0$ of the set H_0 in the space G. It is not hard to see that $\overline{H}_0$ is a central subgroup of the group G. Since all the central elements which are in the neighborhood of the identity are contained in H', it follows that $\overline{H}_0$ and H'_0 coincide in the neighborhood of the identity. Suppose now that a certain point $z \varepsilon \overline{H}_0$ does not belong to H_0. Then zH'_0 forms a neighborhood of this point in $\overline{H}_0$, and therefore there exists an element $y \varepsilon H$ such that $y \varepsilon z H'_0$. But in that case $z \varepsilon y\ H_0'^{-1}$, i.e., $z \varepsilon H_0$. In this way $\overline{H}_0 = H_0$ and hence H_0 is closed in G.

We now denote by H' the local subgroup of the group G which is the direct product of the local subgroups $H'_1, \cdots, H'_k$. We note that H' has no center. It is obvious, furthermore, that the factor group G/H_0 is compact and is locally isomorphic with H'. In this way G/H_0 is a compact semi-simple group (see C)). Therefore a complete connected simply-connected Lie group H which contains the local group H' as one of its neighborhoods of the identity is compact (see Theorem 80). We denote by H_i, $i \geqq 1$, a complete connected simply-connected Lie group containing the local subgroup H'_i as one of its neighborhoods of the identity. It can readily be seen that the direct product H^* of all the groups $H_1, \cdots, H_k$ is simply-connected (see Theorem 60) and is locally isomorphic with the group H. Hence the group H^* is isomorphic with the group H (see Theorem 63), i.e. the group H is decomposable into a direct product of compact, simple, simply-connected Lie groups.

Since H' is a local group of the whole group H, there exists a natural local isomorphism φ' of the group H in the group G which can be extended into an isomorphism φ of the entire group H on the entire group G (see Theorem 63). We now form the direct product G^* of the groups H_0 and H. Every element $g^* \varepsilon G^*$ represents a pair $g^* = (h, h_0)$, where $h \varepsilon H$ and $h_0 \varepsilon H_0$. We associate with the pair $g^*(h, h_0)$ the element $\psi(g^*) = \varphi(h)h_0$. It is not hard to see that the mapping ψ is a homomorphic mapping of the group G^* on the group G, which becomes isomorphic in the neighborhood of the identity. Hence G is isomorphic with the factor group G^*/N, where N is a discrete normal subgroup of the group G^*.

The group H_0 is a connected commutative Lie group. It remains to show that it decomposes into the direct product of one-dimensional Lie groups $K_1, \cdots, K_l$. This is done in the following proposition D). One could refer here to Theorem 44 of Chapter V.

The proof of proposition D) will complete the proof of Theorem 87.

D) Let G be a connected commutative Lie group. Then G decomposes into the direct product of subgroups isomorphic with the group D and subgroups isomorphic with the group K, where D is the additive topological group of real numbers and K is its factor group with respect to the subgroup of integers. If G is compact, then the direct cofactors which are isomorphic with D are absent.

Let R be the r-dimensional vector group. It is obvious that R is simply-connected and since the groups G and R are locally isomorphic (see Example 56), it follows that R is a universal covering group for the group G (see Definition 44). In this way the group G is isomorphic with the factor group R/N, where N is a discrete subgroup of the group R (see Theorem 61). Hence we have reduced this investigation to the study of a discrete subgroup N of the vector group R.

We shall show that N contains a system of $s \leqq r$ elements

(6) $$x_1, \quad , x_s$$

which are linearly independent in the vector space R, and are such that every element of N can be represented in the form

(7) $$a_1x_1 + \quad \cdot \cdot + a_sx_s,$$

where $a_1, \cdots, a_s$ are integers.

We shall construct the system (6) by induction. We shall suppose that N contains a system

(8) $$y_1, \cdots, y_k$$

of linearly independent vectors having the following properties: If we denote by P_k the set of all elements of R which can be written in the form

(9) $$d_1y_1 + \cdot \quad + d_ky_k, \quad 0 \leqq d_i \leqq 1,\ i = 1, \cdots, k,$$

where $d_1, \cdots, d_k$ are real numbers, then every element of P_k which belongs to N can be represented by the form (9) with integral coefficients. This means that only the vertices of the parallelopiped P_k belong to N. We shall now show that two cases are possible for the system (8): a) the system (8) is already the system (6), b) the system (8) can be enlarged by adjoining a single element of N in such a way that the hypothesis of the induction holds for this enlarged system.

We denote by R_k the set of all elements of R which can be represented in the form

(10) $$d_1y_1 + \cdot \cdot \quad + d_ky_k,$$

where $d_1, \cdots, d_k$ are arbitrary real numbers, and by N_k the set of all elements of N which can be written in the form

(11) $$a_1y_1 + \cdots + a_ky_k,$$

where $a_1, \cdots, a_k$ are arbitrary integers. We shall show first of all that $N_k = N \cap R_k$. In fact any element x of R_k can be written in the form $x = x' + x''$, where $x' \varepsilon P_k$, and $x'' \varepsilon N_k$. If now $x \varepsilon N$, then $x - x'' = x'$ also belongs to N. But x' also belongs to P_k. Hence x' can be represented by the form (9) with integral coefficients. But x'' on the other hand can be represented by the form (11) with integral coefficients. Therefore $x \varepsilon N_k$, and hence $N_k = N \cap R_k$. If $N \subset R_k$, we get $N = N_k$, i.e., we have case a). If N is not contained in R_k we introduce into R the Euclidean metric. Since P_k is compact and the subgroup N is discrete, it is obvious that the set $N - R_k$ cannot contain elements arbitrarily close to the set P_k. Therefore the distance ρ between the set $N - R_k$ and the set P_k is positive. We shall show that the distance between the sets $N - R_k$ and R_k is also equal to ρ. Let us suppose the contrary to be true, i.e., that there exist elements $z \varepsilon N - R_k$ and $x \varepsilon R_k$ whose distance is less than ρ. We have $x = x' + x''$, where $x' \varepsilon P_k$, $x'' \varepsilon N_k$. Then the distance between the elements $z - x'' \varepsilon N - R_k$ and $x' \varepsilon P_k$ is also less than ρ, which is impossible. We denote by y_{k+1} an element of $N - R_k$ whose distance from R_k is equal to ρ. It is not hard to see that the system

$$y_1, \cdots, y_k, y_{k+1}$$

now satisfies the hypothesis of the induction, i.e., we have case b).

In order to start the induction, at $k = 0$, it is sufficient to let $N_0 = R_0 = P_0 = \{0\}$.

Since the dimension of the space R is finite, the extension of the system (8) cannot continue indefinitely, and we shall finally arrive at case a). Therefore the system (6) exists.

We shall now enlarge the system (6) until it becomes a complete linearly independent system $x_1, \cdots, x_s, x_{s+1}, \cdots, x_r$, and we shall take the vectors of this system as the basis of the space R. The subgroup N has a special form in the coordinates thus defined, from which the decomposition of the group G into the desired direct product follows directly.

Example 74. Making use of Weyl's theorem (see Theorem 80), which remains unproved in this book, and of the results of the present section, we can give a complete analysis of the structure of a connected compact group of finite dimension (see §45).

Every connected compact topological group G of finite dimension which satisfies the second axiom of countability can be obtained in the following way. Let H be a connected simply-connected compact semi-simple Lie group, and let H_0 be a connected compact commutative group of finite dimension. We form the direct product G^* of the groups H and H_0, and then the factor group $G^*/N = G$, where N is a finite normal subgroup of the group G^*. It turns out that for a proper choice of the groups H and H_0 and also of the normal subgroup N, this method will give the preassigned group G.

Comparing this proposition with Theorem 87 we see that for the case of compact groups the only difference between the structure of a general topological

group and that of a Lie group consists in the commutative factor H_0, which, as we have pointed out in Chapter 5, can have a very complicated set-theoretical structure.

In order to prove the above proposition we make use of Theorem 55. By this theorem some neighborhood U of the identity of the group G decomposes into the direct product of a local Lie group L' and a 0-dimensional central normal subgroup Z, while the set of all finite products of elements belonging to L' is everywhere dense in G. On forming the factor group G/Z we obtain a compact Lie group, and the group L' is mapped isomorphically on some neighborhood of the identity of the group G/Z. In this way the local Lie group L' decomposes into the direct product of a local semi-simple group H' and the center H_0'. The simply-connected entire group H which contains H' as a neighborhood of the identity is compact. Just as in the proof of theorem 87 we denote by φ' the local isomorphism of the group H in the group G. It can readily be seen that the isomorphism φ' can be extended into an isomorphism φ of the whole group H in the group G. We denote by H_0^* the set of all finite products of elements belonging to H_0', and by H_0 the closure of the set H_0^* in the space G. Let G^* be the direct product of the groups H and H_0. We associate with every element $g^* = (h, h_0) \in G^*$ the element $\psi(g^*) = \varphi(h)h_0 \in G$. It is not hard to see that ψ is a homomorphic mapping of the group G^* on the group G, whose kernel of homomorphism is finite.

56. Transformation Groups

As we have noted before, the concept of a Lie group originally arose in the consideration of groups of continuous transformations. We shall first give the fundamental results of the theory of groups of continuous transformations in its classical local form, and then we shall stop somewhat to consider the theory in the large.

In local considerations, which are usual for the classical approach, all the functions under consideration are defined not for all values of the variables, but only in some definite region. Therefore an accurate account would necessitate the definition of the region of existence of every function used. We shall not stop here to define these regions, as it is not hard to determine the sufficiently small regions in which each of these functions is defined.

DEFINITION 47. Let G be an r-dimensional Lie group, and Γ an open set of the n-dimensional Euclidean space. Suppose that to every element $x \in G$ corresponds a transformation φ_x of the open set Γ which associates with an element $\xi \in \Gamma$ some element $\eta \in \Gamma$:

$$\eta = \varphi_x(\xi) = \varphi(\xi, x). \tag{1}$$

We shall say that G is a *transformation group* of the manifold Γ if the following conditions are fulfilled: a)

$$\varphi_x(\varphi_y(\xi)) = \varphi_{xy}(\xi), \tag{2}$$

i.e., the product of the elements corresponds to the product of the transformations. From this it follows, in particular, that to the identity e corresponds the identical transformation φ_e:

(3) $$\varphi_e(\xi) = \xi.$$

b) Two transformations φ_x and φ_y coincide only if $x = y$. This is equivalent to requiring that the transformation φ_x be the identity only when x is the identity e of the group G.

c) In what follows we shall suppose that the function $\varphi(\xi, x)$, as a function of the coordinates of the point ξ and the element x, is differentiable a sufficient number of times.

Relation (1) becomes in coordinate form

(4) $$\eta^i = \varphi_x^i(\xi) = \varphi^i(\xi, x) = \varphi^i(\xi^1, \cdots, \xi^n; x^1, \cdots, x^r), \qquad i = 1, \cdots, n.$$

A) Let G be a transformation group of the manifold Γ and $x(t)$ a curve in G having the direction vector a (see §38, B)). The point $\varphi(\xi, x(t))$ describes for a fixed ξ a curve in the manifold Γ. The vector tangent to the curve $\varphi(\xi, x(t))$ at the point $t = 0$ does not depend on the curve $x(t)$ itself, but is defined by the vector a only. We therefore denote this tangent vector by $\psi(\xi, a)$. In coordinate form this vector $\psi(\xi, a)$ can be expressed as follows:

(5) $$\psi^i(\xi, a) = \lambda_\alpha^i(\xi)a^\alpha = \lambda_\alpha^i(\xi^1, \cdots, \xi^n)a^\alpha,$$

where

(6) $$\lambda_j^i(\xi) = \frac{\partial\varphi^i(\xi, x)}{\partial x^j} \quad \text{for} \quad x = e$$

(see (4)). The function $\eta = \varphi(\xi, x)$ taken as a function of x for a fixed ξ can be defined by the following system of differential equations (see (6)):

(7) $$\frac{\partial\eta^i}{\partial x^j} = \lambda_\alpha^i(\eta)v_j^\alpha(x),$$

where $v_j^\alpha(x)$ are the auxiliary functions of the group G (see §51, A)). The integrability conditions for the system (7) are of the form (see Theorem 69)

(8) $$\frac{\partial\lambda_j^i(\eta)}{\partial\eta^\alpha}\lambda_k^\alpha(\eta) - \frac{\partial\lambda_k^i(\eta)}{\partial\eta^\alpha}\lambda_j^\alpha(\eta) = c_{jk}^\beta\lambda_\beta^i(\eta)$$

where the c_{jk}^β are the structural constants of the group G.

We shall first prove relations (5). Differentiating relation (4) with respect to t we get, by putting $x = x(t)$,

$$\frac{d\varphi^i(\xi, x(t))}{dt} = \frac{\partial\varphi^i(\xi, x)}{\partial x^\alpha}\frac{dx^\alpha}{dt}.$$

For $t = 0$, this last relation gives (5).

In order to prove (7) we introduce, as in §51 (see §51, A)) the element $p = (x + \delta x)x^{-1}$. We then have

$$\varphi(\xi, x + \delta x) = \varphi(\eta, \rho)$$

(see (1) and (2)). Passing from finite increments to derivatives we get relation (7) (see §51, A)).

By Theorem 69, the integrability conditions of system (7) have the form

$$\frac{\partial \lambda^{i}_{\alpha}(\eta)}{\partial \eta^{\gamma}} v^{\alpha}_{j}(x)\lambda^{\gamma}_{\beta}(\eta)v^{\beta}_{k}(x) - \frac{\partial \lambda^{i}_{\beta}(\eta)}{\partial \eta^{\gamma}} v^{\beta}_{k}(x)\lambda^{\gamma}_{\alpha}(\eta)v^{\alpha}_{j}(x) + \lambda^{i}_{\delta}(\eta)\left(\frac{\partial v^{\delta}_{i}(x)}{\partial x^{k}} - \frac{\partial v^{\delta}_{k}(x)}{\partial x^{j}}\right) = 0.$$

Making use of relation (8) of §51, we can write the last relation in the form

$$(9) \qquad \left(\frac{\partial \lambda^{i}_{\alpha}(\eta)}{\partial \eta^{\gamma}} \lambda^{\gamma}_{\beta}(\eta) - \frac{\partial \lambda^{i}_{\beta}(\eta)}{\partial \eta^{\gamma}} \lambda^{\gamma}_{\alpha}(\eta) - \lambda^{i}_{\delta}(\eta)c^{\delta}_{\alpha\beta}\right) v^{\alpha}_{j}(x)v^{\beta}_{k}(x) = 0.$$

Since the determinant of the matrix $\|v^{\alpha}_{j}(x)\|$ is distinct from zero, it is not hard to see that relations (8) and (9) are equivalent.

B) Let G be a group of continuous transformations of the manifold Γ and R the infinitesimal group of the group G. In A) we associated with every vector $a \,\varepsilon\, R$ a vector field $\psi(\xi, a)$ defined in the manifold Γ. In this way we have a family P of vector fields of the form $\psi(\xi, a)$ defined on Γ. It follows directly from relation (5) that if α and β are real numbers, then

$$(10) \qquad \psi(\xi, \alpha a + \beta b) = \alpha\psi(\xi, a) + \beta\psi(\xi, b).$$

Hence if the vector fields λ and μ belong to the family P, then the vector field $\alpha\lambda + \beta\mu$ also belongs to P. This means that the family P is a vector space under addition. We define in the family P the commutator of two of its elements $\lambda = \lambda(\xi)$ and $\mu = \mu(\xi)$ by letting

$$(11) \qquad [\lambda(\xi), \mu(\xi)]^{i} = \frac{\partial \lambda^{i}(\xi)}{\partial \xi^{\gamma}} \mu^{\gamma}(\xi) - \frac{\partial \mu^{i}(\xi)}{\partial \xi^{\gamma}} \lambda^{\gamma}(\xi).$$

Then the following relation holds:

$$(12) \qquad [\psi(\xi, a), \psi(\xi, b)] = \psi(\xi, [a, b]).$$

Relation (12) shows that if $\lambda \,\varepsilon\, P$ and $\mu \,\varepsilon\, P$, then also $[\lambda, \mu] \,\varepsilon\, P$. This defines the operation of commutation in P. It follows from relations (10) and (12) that in passing from a vector $a \,\varepsilon\, R$ to the vector field $\psi(\xi, a) \,\varepsilon\, P$ the operations of addition, multiplication by a real number, and commutation are preserved. This shows that the operation of commutation established in P satisfies the conditions of Definition 46, and that the mapping ψ which associates the field $\psi(\xi, a) \,\varepsilon\, P$ with the vector $a \,\varepsilon\, R$ is a homomorphic mapping of the infinitesimal group R on the infinitesimal group P. It appears moreover that the mapping ψ

is not only homomorphic, but is also isomorphic. We shall call the infinitesimal group P an *infinitesimal group of transformations* of the manifold Γ. Relation (10), as we have already indicated, follows directly from (5). In order to prove (12) we multiply both sides of (8) by $a^j b^k$ and sum over j and k. The relation thus obtained gives (12) by making use of (5).

In order to establish the isomorphism of the mapping ψ it is sufficient to show that the dimension of the vector space P is equal to the dimension r of the space R. We denote by $\lambda_k(\xi)$ the vector field having the components $\lambda_k^1(\xi), \cdots, \lambda_k^n(\xi)$. The vector fields

$$\lambda_k(\xi), \qquad k = 1, \cdots, r, \tag{13}$$

form a basis of the space P (see (5)). Therefore it will suffice to show that the vector fields (13) are linearly independent, i.e., a linear combination of these vector fields with constant coefficients is zero only if all the coefficients are zero.

We now consider in G a certain one-parameter subgroup $x(t)$ having the direction vector a. We substitute $x(t)$ for t in (7), multiply the resulting equation by $dx^j(t)/dt$ and sum over j. We get

$$\frac{d\eta^i}{dt} = \lambda_\alpha^i(\eta) v_j^\alpha(x(t)) \frac{dx^j(t)}{dt} = \lambda_\alpha^i(\eta) a^\alpha \tag{14}$$

(see §51, (9)). If we now suppose that the vector fields of the system (13) are linearly dependent, then there exists a vector $a \neq 0$ such that the right side of relation (14) is identically zero. This shows that $\eta = \varphi(\xi, x(t))$ is a constant, i.e., $\eta = \xi$. Hence to the element $x(t)$ distinct from the identity corresponds the identical transformation, which is impossible (see Definition 47). Hence B) is completely established.

The converse of propositions A) and B) is found in the following theorem.

THEOREM 88. *Let Γ be an n-dimensional open set of Euclidean space. Suppose an r-dimensional linear family P of vector fields is defined on Γ.* (*Linearity* of the family P means that if two vector fields $\lambda(\xi)$ and $\mu(\xi)$ are in P, then P also contains the field $\alpha\lambda(\xi) + \beta\mu(\xi)$, where α and β are real numbers.) *We introduce into P the operation of commuation by putting*

$$[\lambda(\xi), \mu(\xi)]^i = \frac{\partial\lambda^i(\xi)}{\partial\xi^\gamma}\mu^\gamma(\xi) - \frac{\partial\mu^i(\xi)}{\partial\xi^\gamma}\lambda^\gamma(\xi). \tag{15}$$

We suppose that if the vector fields λ and μ are in P, then the vector field $[\lambda, \mu]$ is also in P. Under these conditions we shall say that an infinitesimal group of transformations P is defined on Γ. It turns out that there exists one and only one local Lie group G of continuous transformations of the manifold Γ (see A) *such that the infinitesimal group of transformations which corresponds to it* (see C)) *coincides with the preassigned infinitesimal group P.*

PROOF. We note first of all that if λ, μ, ν are three vector fields, then the following relations hold:

$$[\lambda, \mu] + [\mu, \lambda] = 0 \tag{16}$$

$$[\lambda, [\mu, \nu]] + [\mu, [\nu, \lambda]] + [\nu, [\lambda, \mu]] = 0 \tag{17}$$

These relations can be verified by direct calculations from the defining relation (15).

We now select r linearly independent vector fields $\lambda_k(\xi)$ $k = 1, \cdots, r$, in P. Such a system exists and forms a basis of the family P, since the dimension of the family is r by assumption. We therefore have

$$[\lambda_j(\xi), \lambda_k(\xi)] = c_{jk}^{\gamma}\lambda_\gamma(\xi), \tag{18}$$

where the c_{jk}^i are constants which in view of relations (16) and (17) satisfy the usual relations holding for structural constants (see §48, (11) and (12)). We construct from the structural constants c_{jk}^i the local Lie group G (see Theorem 72), and denote its auxiliary functions by $v_j^i(x)$.

We now consider the system of equations

$$\frac{\partial \eta^i}{\partial x^j} = \lambda_\alpha^i(\eta)v_j^\alpha(x) \tag{19}$$

with respect to an unknown function η of the element x. We have already considered a system of this type (see (7)) and have shown that its integrability conditions are of the form (8). But (18) is merely another form of (8), so that the system (19) is integrable. We denote by $\varphi(\xi, x)$ the solution of the system (19) which satisfies the initial condition

$$\varphi(\xi, e) = \xi. \tag{20}$$

In this way we have associated with every element $x \in G$ a transformation φ_x of the manifold Γ which transforms the point $\xi \in \Gamma$ into the point $\eta = \varphi_x(\xi) = \varphi(\xi, x) \in \Gamma$. We shall show that conditions a) and b) of Definition 47 hold here.

Let x and y be two elements of G. We shall consider y as fixed and x as variable. Let

$$f = xy, \qquad \eta = \varphi(\xi, y), \qquad \zeta^* = \varphi(\eta, x), \qquad \zeta = \varphi(\xi, f).$$

In order to show that condition a) holds it is sufficient to show that $\zeta^* = \zeta$. In order to do this we proceed in the usual way and show that the functions ζ^* and ζ of the element x satisfy the same system of differential equations with the same initial conditions $\zeta^*(e) = \zeta(e) = \eta$.

We have

$$\frac{\partial \zeta^{*i}}{\partial x^j} = \lambda_\alpha^j(\zeta^*)v_j^\alpha(x) \tag{21}$$

(see (7)). We denote by $\|u_j^i(x)\|$ the matrix inverse to the matrix $\|v_j^i(x)\|$. Then relation (6) of §51 is transformed into

$$\frac{\partial f^{\alpha}}{\partial x^{j}} = u_{\beta}^{\alpha}(f)v_{j}^{\beta}(x). \tag{22}$$

From relations (22) we have

$$\frac{\partial \zeta^{i}}{\partial x^{j}} = \frac{\partial \zeta^{i}}{\partial f^{\alpha}}\frac{\partial f^{\alpha}}{\partial x^{j}} = \lambda_{\gamma}^{i}(\zeta)v_{\alpha}^{\gamma}(f)u_{\beta}^{\alpha}(f)v_{j}^{\beta}(x) = \lambda_{\alpha}^{i}(\zeta)v_{j}^{\alpha}(x). \tag{23}$$

But systems (21) and (23) coincide. Hence because of the uniqueness of the solution of the system, satisfying given initial conditions, we have $\zeta^{*} = \zeta$ and hence condition a) is fulfilled.

In order to prove that b) holds, let us suppose on the contrary that b) does not hold. Then there exists a normal subgroup N of the group G to all of whose elements correspond identical transformations of the manifold Γ. We can conclude from this that there exists a one-parameter subgroup $x(t)$ to whose elements correspond identical transformations of the manifold Γ, and which has a direction vector a distinct from zero.

Substituting $x(t)$ for t in relation (19), multiplying by $dx^{j}(t)/dt$ and summing, we get

$$\frac{d\eta^{i}}{dt} = \lambda_{\alpha}^{i}(\eta)v_{\beta}^{\alpha}(x(t))\frac{dx^{\beta}(t)}{dt} = \lambda_{\alpha}^{i}(\eta)a^{\alpha} \tag{24}$$

(see 51, (9)). Since $\eta(t)$ is a fixed point by assumption, the left side of relation (24) becomes zero, and we get the identity

$$\lambda_{\alpha}^{i}(\xi)a^{\alpha} = 0.$$

This show that the vector fields $\lambda_{k}(\xi)$, $k = 1, \cdots, r$, are linearly dependent, which contradicts our assumption.

It is obvious that c) holds since the function $\varphi(\xi, x)$ is obtained as a result of integrating a system of equations. Hence Theorem 88 is proved.

We now consider a special type of transformation groups, namely the transitive groups.

C) Let G be a transformation group of the manifold Γ. The group G is called *transitive* if for any two points p and q of the manifold Γ there exists an element x of the group G such that $\varphi_{x}(p) = q$. (We should not forget here that due to the local nature of the whole consideration the element x may exist only for points p and q which are sufficiently close to each other.) Let a be a fixed point of the manifold Γ. We denote by K_{p} the totality of elements $x \varepsilon G$ for which $\varphi_{x}(a) = p$. Then $H = K_{a}$ is a subgroup of the group G, and K_{p} is a left coset of the subgroup H in the group G. Moreover the group H contains no normal subgroup of the group G distinct from the identity. If K is a left coset of the subgroup H in the group G, then for $x \varepsilon K$, $y \varepsilon K$, we have $\varphi_{x}(a) = \varphi_{y}(a)$. Hence $\varphi_{x}(a)$ is a definite point $q \varepsilon \Gamma$, which depends on the class K containing x, but not on the element x itself, i.e., $K = K_{q}$. We have

therefore established a one-to-one correspondence between points of the manifold Γ and left cosets of the subgroup H in the group G. If furthermore

$$\varphi_k(p) = q, \tag{25}$$

then

$$xK_p = K_q. \tag{26}$$

Hence if we know the group G and its subgroup H we can obtain the manifold Γ as a manifold of cosets, and then define transformations in this manifold by means of relations (25) and (26).

If we are given independently of the manifold Γ a certain local group G and a subgroup H of G which contains no normal subgroup of the group G distinct from the identity, then by the above method we can construct a manifold Γ and define in it in a natural way the transitive transformation group G. The manifold Γ will be defined as the set of left cosets of the subgroup H in the group G, and the transformation φ_x will be defined by the relations $\varphi_x(K) = xK$, where $K \varepsilon \Gamma$.

The above shows that the consideration of a transitive transformation group is entirely equivalent to the consideration of a local Lie group G and a subgroup H of G which contains no normal subgroup of the group G distinct from the identity. As long as we confine ourselves to a local investigation, the group G and its subgroup H may be defined by the corresponding infinitesimal group R and its subgroup S. Hence the local study of a transitive transformation group is reduced to the study of an elementary algebraic subject, namely the infinitesimal group R together with a subgroup S of R which contains no normal subgroup of R distinct from zero.

In particular, in order to classify the transitive transformation groups it is sufficient to classify all the pairs R, S.

I do not give here the proof of proposition C), but this proof presents no difficulties.

D) Let G be a transitive transformation group of the manifold Γ (see (Definition 47, and C)). Then we can introduce analytic coordinates in G and Γ, i.e., a system of coordinates in which the functions (4) are analytic functions of all of their variables.

In order to prove D) we shall interpret the points of the manifold Γ as left cosets of a subgroup H in the group G (see C)). We introduce first of all canonical coordinates of the second kind in G (see §40, A)), by taking as their basis the one-parameter subgroups $h_k(t)$, $k = 1, \cdots, r$. These subgroups we shall select in such a way that $h_{n+1}(t), \cdots, h_r(t)$ are in H and their products cover H. Every element $z \varepsilon G$ can now be written in the form $z = h_1(t^1) \cdots h_n(t^n)h_{n+1}(t^{n+1}) \cdots h_r(t^r)$. If the coordinates $t^1, \cdots, t^n$ are fixed, while the remaining coordinates assume arbitrary values, then the element z will describe a certain left coset K. We shall take for the coordinates of the coset K the numbers $t^1, \cdots, t^n$. Since the points of the manifold Γ

have been interpreted by us as cosets, this defines a definite system of coordinates in the manifold Γ. Let

$$x = h_1(x^1) \cdots h_r(x^r)$$

be an arbitrary element of the group G and

$$\xi = h_1(\xi') \quad h_n(\xi^h)h_{n+1}(s^{n+1}) \cdot \quad (h_r(s^r)$$

be an arbitrary coset. In order to define the coset $\varphi_x(\xi) = \eta$ we form the product

$$\begin{aligned}\eta &= \varphi_x(\xi) = \varphi(\xi, x) = x\xi \\ &= h_1(x^1) \cdots h_r(x^r)h_1(\xi^1) \cdots h_n(\xi^n)h_{n+1}(s^{n+1}) \cdots h_r(s^s) \\ &= h_1(\eta^1) \qquad h_n(\eta^n)h_{h+1}(t^{n+1}) \qquad h_r(t^r).\end{aligned}$$

If x and ξ are given, the coset $\varphi_x(\xi) = \eta$ is also given, and hence $\eta^i = \varphi^i(\xi, x)$, $i = 1, \cdots, n$, i.e., η^i does not depend on the arbitrary coordinates $s^{n+1}, \cdots, s^r$. Since the canonical coordinates of the second kind are analytic (see Theorem 72 and §40, A)), the functions $\varphi^i(\xi, x)$ are analytic functions. Hence D) is established.

So far we have considered only the local aspects of a transformation. The concept of a transformation group in the large is defined in a natural way analogous to Definition 47. One does not suppose in this case that the manifold Γ is a region of Euclidean space. The statements of remark C) are carried over to the transformation groups in the large. In fact we have the following proposition.

E) Let G be an entire Lie group and H a subgroup of G which contains no subgroup of the group G distinct from the identity. The set of left cosets of the subgroup H in the group G forms a manifold Γ. We now associate with every element $x \in G$ a transformation φ_x of the manifold Γ by letting $\varphi_x(K) = xK$, where $K \in \Gamma$. From this construction we get a transitive transformation group G of the manifold Γ. It is not hard to show that every transitive Lie group of transformations can be obtained in this way. Hence the study of the entire transitive Lie group of transformations is reduced to the study of the pair G, H.

Now the question arises: Is it always possible to extend a given local group of transformations into a transformation group? It appears that this is not always possible. I give here an example to the contrary.

EXAMPLE 75. We constructed in Example 68 an entire simply-connected Lie group G and a one-dimensional local subgroup H of G such that H contains no one-dimensional entire subgroup of the group G. It follows from Theorem 85 that H is not a normal subgroup of the group G, and being one-dimensional H contains no normal subgroup. If G' is a neighborhood of the identity of the group G then the local group G' together with its subgroup H defines a locally transitive group of transformations (see C)). But it is not possible to extend this group of transformations into an entire group, since H cannot be contained in an entire one-dimensional subgroup of the group G.

BIBLIOGRAPHY

1. Ado, I. On the Representation of Finite Continuous Groups by Means of Linear Substitutions. Izvestia Kazan, v. 7, pp. 3–43, 1934–35, (in Russian).
2. Alexandroff, P. and Efremovich, V. On the Fundamental Concepts of Topology, Moscow, 1936, (in Russian).
3. Alexandroff, P. and Hopf, H. Topologie, Berlin, 1936.
4. Bochner, S. and Neumann, J. von. Almost periodic Functions in Groups, II. Trans. of Amer. Math. Soc. v. 37, pp. 21–50, 1935.
5. Cartan, E. Sur la structure des Groupes de Transformations Finis et Continus, Paris Dissertation, 1894.
6. Cartan, E. Groupes Simples Clos et Ouverts et Géometrie Riemannienne Jour. Math. pure and appl. v. 8, pp. 1–33, 1929.
7. Cartan, E. La Théorie des Groupes Finis and Continus et l'Analysis Situs. Mem. Sci. Math. fasc. XLII, 1930.
8. Dantzig, D. van. Über Topologisch Homogene Kontinua. Fund. Math. v. 14, pp. 102–125, 1930.
9. Dantzig, D. van. Zur Topologischen Algebra, I, Math. Ann. v. 107, pp. 587–626, 1932.
10. Dantzig, D. van. Zur Topologischen Algebra, II. Comp. Math. v. 2, pp. 201–223, 1935.
11. Haar, A. Der Massbegriff in der Theorie der kontinuierlichen Gruppen. Ann. of Math. v. 34, pp. 147–169, 1933.
12. Hausdorff, F. Grundzüge der Mengenlehre, 1914.
13. Kampen, E. van. Locally compact Abelian Groups. Proc. Nat. Acad. Sc. v. 20, pp. 434–436, 1934.
14. Kampen, E. van. The Structure of a Compact Connected Group. Am. Jour. Math. v. 57, pp. 301–308, 1935.
15. Kampen, E. van. Locally Bicompact Abelian Groups and their Character Groups. Ann. of Math. v. 36, pp. 448–463, 1935.
16. Kampen, E. van. Note on a Theorem of Pontrjagin. Amer. Jour. of Math. v. 58, pp. 177–180, 1936.
17. Lardy, P. Sur la Détermination des Structures Réelles de Groupes Simples, Finis et Continus, au moyen des Isomorphies Involutives. Comm. Math. Helvet. v. 8, pp. 189–234, 1935–36.
18. Levi, E. Sulla Struttura die Gruppi Finiti e Continici, Atti. Accad. Torino, v. 40, pp. 3–17, 1905.
19. Lie, S. und Engel, F. Theorie der Tranformations gruppen. Leipzig, vs. 1, 2, and 3.
20. Markoff, A. Über endlich-dimensionale Vektorräume. Ann. of Math. v. 36, pp. 464–506, 1935.
21. Neumann, J..von. Die Einführung analytischer Parameter in topologischen Gruppen, Ann. of Math. v. 34, pp. 170–190.

22. Neumann, J. von. Zum Haarschen Mass in Topologischen Gruppen Comp. Math. v. 1, 1934.
23. Neumann, J. von. Almost periodic Functions in Groups I. Trans. Amer. Math. Soc. v. 36, pp. 445–492, 1934.
24. Peter, F. and Weyl, H. Die Vollständigkeit der Primitiven Darstellungen einer Geschlossenen Kontinuierlichen Gruppe. Math. Ann. v. 97, pp. 737–755, 1927.
25. Pontrjagin, L. Über stetige algebraische Körper. Ann. of Math. v. 33, pp. 163–174, 1932.
26. Pontrjagin, L. Sur les Groupes Topologiques Compactes et la Cinquième Problème de M. Hilbert. C. R. Paris, v. 198, pp. 238–240, 1934.
27. Pontrjagin, L. Sur les Groupes Abéliens Continus. C. R. Paris, v. 198, pp. 328–330, 1934.
28. Pontrjagin, L. The Theory of Topological Commutative Groups. Ann. of Math. v. 35, pp. 361–388, 1934.
29. Pontrjagin, L. Linear Representations of Compact Topological Groups. Mat. Sbornick (new series) v. 1, pp. 267–271, 1936.
30. Pontrjagin, L. The Structure of Continuous Groups, a report to the Second United Mathematical Congress, the Academy of Sciences, Moscow, pp. 237–257, 1936 (in Russian).
31. Schreier, O. Abstrakte Kontinuierliche Gruppen, Hamburg Abh. Math. Sem. v. 4, pp. 15–32, 1925.
32. Schreier, O. Die Verwandschaft Stetiger Gruppen im Grossen, Hamburg Abh. Math. Seminar. v. 5, pp. 233–244, 1926.
33. Waerden, B. van der. Moderne Algebra, i., ii. Julius Springer, Berlin, 1930.
34. Waerden, B. van der. Die Klassifikation der einfachen Lieschen Gruppen. Math. Ztschr. v. 37, pp. 446–462, 1933.
35. Weyl, H. Theorie der Darstellung kontinuierlicher halb-einfacher Gruppen durch Lineare Transformationen, I. Math. Ztschr. v. 23, pp. 271–304, 1924, II. and III, v. 24, pp. 328–395, 1925.
36. Whitehead, J. H. C. On the Decomposition of an Infinitesimal Group. Proc. Cambr. Phil. Soc., v. 32, pp. 229–237, 1936.

The References to Literature by Chapters.

Introduction. [12].
Chapter I. [33].
Chapter II. [3].
Chapter III. [8], [9], [10], [20].
Chapter IV. [4], [11], [22], [23], [24], [29].
Chapter V. [8], [13], [15], [20], [25], [27], [28].
Chapter VI. See Chapter 9.
Chapter VII. [2], [14], [16], [21], [26].
Chapter VIII. [31], [32].
Chapter IX. [1], [5], [6], [7], [17], [18], [19], [34], [35], [36].
A general survey of the theory of topological Groups [30].
A general survey of the theory of Lie Groups [7].

INDEX